



Deployment Guide

Avaya 3100 Mobile Communicator

3.1
NN42030-301, 01.04
October 2010

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: <http://www.avaya.com/support>. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://support.avaya.com/licenseinfo/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be

accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://www.avaya.com/support/Copyright/>.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: <http://www.avaya.com/support>

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://www.avaya.com/support>

Contents

Chapter 1: New in this release.....	7
Features.....	7
Other changes.....	7
Chapter 2: Introduction.....	9
References.....	9
Chapter 3: Planning and engineering.....	11
Chapter 4: Planning.....	13
Avaya 3100 MC - Client and Avaya 3100 MC - Web UI network deployment.....	13
Avaya 3100 Mobile Communicator Gateway network deployment.....	15
Communication server requirements.....	16
Dialing plans and telephone numbers.....	16
Security requirements.....	18
High availability.....	20
Capacity.....	22
Chapter 5: Engineering.....	23
Client device specifications.....	23
Gateway specifications.....	23
Port tables.....	23
Chapter 6: Interworking requirements with CS 1000.....	29
Avaya CS 1000 deployment considerations.....	29
Avaya CS 1000 Source Based Routing.....	29
Avaya CS 1000 package requirements.....	30
Avaya CS 1000 engineering for Avaya 3100 Mobile Communicator.....	30
SIP Trunk configuration.....	34
Device Handoff configuration.....	35
Avaya CS 1000 system redundancy.....	36
Call Forward No Answer feature interactions.....	36
Avaya CS 1000 capacity requirements.....	37
Trunk calculation: Method 1.....	38
Trunk calculation: Method 2.....	39
UEXT calculations.....	42
Avaya CS 1000 and supported Avaya 3100 Mobile Communicator features.....	42
Call Detail Recording.....	44
Direct outbound call.....	44
Call-Me-First outbound call.....	44
Incoming call.....	44
Chapter 7: Deployment planning.....	47
Navigation.....	47
Licensing requirements.....	48
Avaya 3100 MC - Client and Avaya 3100 MC - Web UI licenses.....	48
Avaya 3100 Mobile Communicator Gateway licenses.....	49
Avaya CS 1000 SIP Gateway CLID Parameters configuration.....	49
Parameter: Country Code.....	51

Parameter: Area Code.....	51
Parameter: Subscriber/Number of Digits to strip.....	51
Parameter: Subscriber/Prefix to insert.....	51
Parameter: National/Number of Digits to strip.....	51
Parameter: National / Prefix to insert.....	52
Mobility prefix.....	52
Data access planning.....	53
Avaya CS 1000 data access considerations.....	53
Service DN.....	53
Universal Extensions.....	54
Caller ID table.....	54
Chapter 8: Deployment work flow.....	57
Deploying the systems task flow.....	57
Chapter 9: Deployment prerequisites.....	59
Establishing the Avaya CS 1000 and Avaya 3100 Mobile Communicator system baseline.....	59
Checking the Avaya CS 1000 release from Element Manager.....	61
Checking the Avaya CS 1000 release from the command line.....	62
Chapter 10: Avaya 3100 Mobile Communicator Gateway installation.....	63
Avaya 3100 Mobile Communicator Gateway installation workflow.....	63
Preparation.....	65
Avaya 3100 Mobile Communicator Gateway preparation workflow.....	65
Installing the Linux base.....	67
Verifying the Enterprise network.....	71
Job aid: Supported LDAP servers.....	71
Installation.....	72
Installation task flow.....	72
Job aid: Admin shell access.....	73
Installing the Avaya 3100 Mobile Communicator Gateway software.....	73
Commissioning.....	74
Adding an Avaya 3100 Mobile Communicator Gateway server.....	74
Configuring the Gateway settings.....	75
Procedure job aid.....	76
Configuring the dial plan conversion parameters.....	81
Variable definitions.....	82
Rules that use the carat sign.....	82
Configuring the device settings.....	83
Procedure job aid.....	84
Configuring the emergency telephone numbers.....	87
Adding the Avaya 3100 Mobile Communicator Gateway license.....	88
Checking Gateway server status.....	89
Procedure job aid.....	90
Solution commissioning.....	92
Chapter 11: Avaya CS 1000 configuration for client support.....	95
Avaya CS 1000 configuration for client support task flow.....	95
Configuring zones.....	97
Configuring a D-channel for virtual trunks.....	97
Configuring virtual routes.....	98
Configuring virtual trunks.....	100

Configuring network control parameters data block.....	101
Configuring ESN access codes.....	101
Configuring the Route List Block.....	102
Coordinated Dialing Plan.....	103
Forwarding Service DN to Avaya 3100 Mobile Communicator Gateway.....	103
Configuring a Handoff key.....	105
Configuring a HOT P key.....	106
Configuring the SIP trunk gateway.....	107
Configuring the SIP Gateway settings.....	109
Configuring the SIP URI to NPI/TON mapping.....	110
Restarting the Signaling Server.....	112
Warm restart.....	112
Cold restart.....	112
Configuring NRS.....	112
NRS Database.....	113
Committing NRS Database.....	113
Configuring Domain names on the NRS.....	114
Configuring gateway endpoints on the NRS.....	116
Adding a User Endpoint.....	119
Job Aid.....	122
Adding an NRS Routing rule for the Avaya 3100 Mobile Communicator Gateway.....	122
Adding an NRS Routing rule for the Avaya CS 1000.....	125
Chapter 12: CallPilot MWI configuration.....	127
MWI for Avaya CS 1000.....	127
Chapter 13: Validate deployment.....	129
Validating deployment task flow.....	129
Validating Avaya 3100 Mobile Communicator Gateway registration.....	130
Job aid.....	130
Validating Avaya 3100 MC - Client for BlackBerry communication.....	131
Validating Avaya 3100 Mobile Communicator and Avaya CS 1000 ECS deployment.....	132
Chapter 14: Upgrade fundamentals.....	135
Navigation.....	135
Upgrade work flow.....	136
Upgrading from Release 2.x to Release 3.0.....	136
Release upgrade taskflow.....	137
Capturing Release 2.x parameters.....	138
Job Aid: Release 2.x parameter worksheet.....	139
Upgrading from Release 3.0 to Release 3.1.....	139
Prerequisites.....	140
Upgrading from Release 3.0 to Release 3.1 taskflow.....	140
Recording the Release 3.0 configuration parameters.....	141
Release 3.0 system configuration job aid.....	142
Upgrading the Avaya 3100 Mobile Communicator Gateway software to a new software release.....	145
Upgrade commissioning.....	147
Upgrading for a Service Upissue.....	147
Upgrading the Avaya 3100 Mobile Communicator system software from CD.....	147
Converting to a redundant configuration.....	148

Chapter 15: Maintenance.....	151
Navigation.....	151
Removing a Service Upissue.....	151
Job Aid.....	152
Uninstalling the Avaya 3100 Mobile Communicator system software.....	152
Chapter 16: Common procedures.....	155
Logging on to the Avaya 3100 Mobile Communicator Web Administration Console as an administrator.....	155
Changing the Avaya 3100 Mobile Communicator Web Administration Console password.....	156
Managing the server processes from the Web Administration Console.....	157
Managing the server processes from the command line.....	158
Accessing the server command line as nortel.....	159
Accessing the server command line as superuser.....	159
Backing up the Avaya 3100 Mobile Communicator Gateway server databases.....	160
Restoring the Avaya 3100 Mobile Communicator Gateway server databases.....	161
Chapter 18: Appendix A: Installation worksheets and checklist.....	163
Linux base worksheet.....	163
Avaya 3100 Mobile Communicator Gateway worksheet.....	164
Avaya 3100 Mobile Communicator solution checklist.....	166
Chapter 18: Appendix B: Call flows from CS 1000.....	169
Index.....	171

Chapter 1: New in this release

This section details what's new in *Avaya 3100 Mobile Communicator Deployment Guide, NN42030-301* for Avaya 3100 Mobile Communicator Release 3.1.

Features

This document is new for Avaya 3100 Mobile Communicator Release 3.1.

For more information about Avaya 3100 Mobile Communicator, see *Avaya 3100 Mobile Communicator Fundamentals, NN42030-109*.

Other changes

This document is new for Avaya 3100 Mobile Communicator Release 3.1. It consolidates the following documents:

- *Avaya 3100 Mobile Communicator Planning and Engineering, NN42030-200*
- *Avaya 3100 Mobile Communicator Installation and Commissioning, NN42030-300*
- *Avaya 3100 Mobile Communicator and Avaya Communication Server 1000 Solution Integration Guide, NN49000-315*

Revision History

October 2010	Standard 01.04. This document is issued to support Avaya 3100 Mobile Communicator Release 3.1. Removed obsolete external references.
July 2010	Standard 01.03. This document is issued to support Avaya 3100 Mobile Communicator Release 3.1. Updated Avaya 3100 Mobile Communicator Gateway installation on page 63 and Upgrading the Avaya 3100 Mobile Communicator Gateway software to a new software release on page 145. Added Converting to a redundant configuration on page 148.
April 2010	Standard 01.02. This document is up-issued to provide correction to procedures.
January 2010	Standard 01.01. This document is issued to support Avaya 3100 Mobile Communicator Release 3.1.

New in this release

Chapter 2: Introduction

This document guides you through the deployment steps for Avaya 3100 Mobile Communicator (Avaya 3100 Mobile Communicator). These steps include planning, engineering, installation of the Avaya 3100 Mobile Communicator, and interworking the Avaya 3100 Mobile Communicator with the Avaya Communication Server 1000 (Avaya CS 1000).

- [Planning and engineering](#) on page 11 takes you through the planning and engineering required. At the end of this step, you will have completed a worksheet with parameters you need for deployment.
- [Deployment work flow](#) on page 57 takes you through the installation of Avaya 3100 Mobile Communicator and interworking it with your ECS.

This document also includes the following related sections:

- [Upgrade fundamentals](#) on page 135
- [Maintenance](#) on page 151
- [Converting to a redundant configuration](#) on page 148
- [Appendix B: Call flows from CS 1000](#) on page 169



Important:

For Avaya CS 1000 platforms, Avaya personnel perform all installation and interworking activities.

References

For more information about Avaya 3100 Mobile Communicator, see *Avaya 3100 Mobile Communicator Fundamentals, NN42030-109*.

For more information about administration tasks and tasks involving the Avaya 3100 Mobile Communicator clients, see *Avaya 3100 Mobile Communicator Administration and Security, NN42030-600*.

For information about the Avaya 3100 Mobile Communicator clients, see

- *Avaya 3100 Mobile Communicator - Client for BlackBerry User Guide, NN42030-101*
- *Avaya 3100 Mobile Communicator - Client for Nokia User Guide, NN42030-102*
- *Avaya 3100 Mobile Communicator - Client for Windows Mobile User Guide, NN42030-107*

- *Avaya 3100 Mobile Communicator - Client for iPhone User Guide, NN42030-111*
- *Avaya 3100 Mobile Communicator - Web UI User Guide, NN42030-110*

Chapter 3: Planning and engineering

This chapter contains information that supports the activities that you must perform before installing an Avaya 3100 Mobile Communicator (Avaya 3100 Mobile Communicator) solution, including requirements, network management, performance, and capacity requirements.

During the planning and engineering phase, use the worksheets in [Appendix A: Installation worksheets and checklist](#) on page 163 to gather the information you need in order to install, configure, and interwork your Avaya 3100 Mobile Communicator with your Avaya Communication Server 1000 (Avaya CS 1000).

- [Planning](#) on page 13
- [Engineering](#) on page 23
- [Interworking requirements with CS 1000](#) on page 29
- [Deployment planning](#) on page 47

Chapter 4: Planning

This chapter details the planning aspects of the Avaya 3100 Mobile Communicator (Avaya 3100 Mobile Communicator).

Navigation

- [Avaya 3100 MC - Client and Avaya 3100 MC - Web UI network deployment](#) on page 13
- [Avaya 3100 Mobile Communicator Gateway network deployment](#) on page 15
- [Communication server requirements](#) on page 16
- [Dialing plans and telephone numbers](#) on page 16
- [Security requirements](#) on page 18
- [High availability](#) on page 20
- [Capacity](#) on page 22

Avaya 3100 MC - Client and Avaya 3100 MC - Web UI network deployment

The Avaya 3100 Mobile Communicator - Client (Avaya 3100 MC - Client) for BlackBerry, the Avaya 3100 MC - Client for Nokia, the Avaya 3100 MC - Client for Windows Mobile, the Avaya 3100 MC - Client for iPhone, and the Avaya 3100 Mobile Communicator - Web UI (Avaya 3100 MC - Web UI) require access to the Avaya 3100 Mobile Communicator Gateway. In this document, the terms Avaya 3100 MC - Client and clients refer to the supported clients and Avaya 3100 MC - Web UI.

The Avaya 3100 MC - Client for BlackBerry supports two network deployment options:

- with the BlackBerry Enterprise Server (BES)
- without the BES

The Avaya 3100 MC - Client for BlackBerry with the BES uses the BES to route data and provide security.

Avaya 3100 MC - Client for BlackBerry (without the BES), Avaya 3100 MC - Client for Nokia, and Avaya 3100 MC - Client for Windows Mobile require a Wireless Access Point or an internet connection through the Enterprise firewall. These clients can also use the cellular data network.

[Figure 1: Typical Avaya 3100 Mobile Communicator network architecture](#) on page 14 shows a typical network architecture.

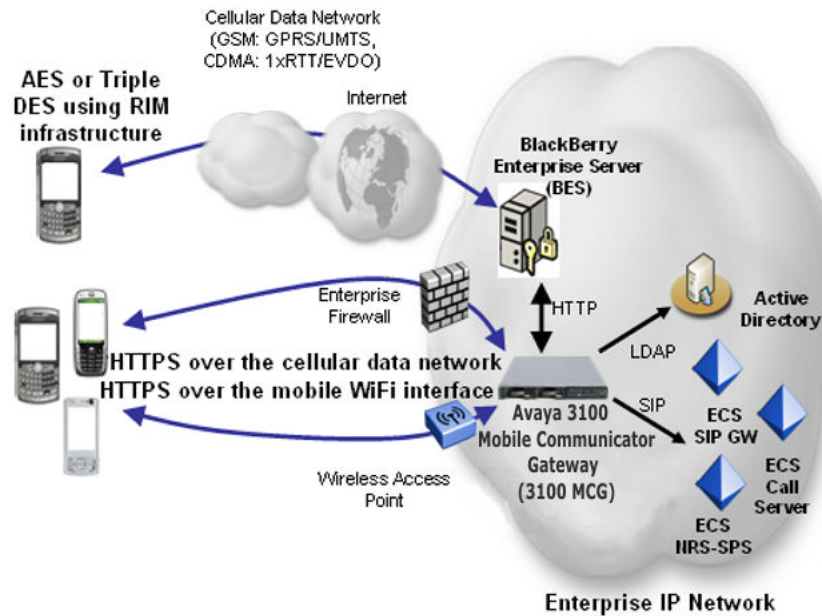


Figure 1: Typical Avaya 3100 Mobile Communicator network architecture

The Avaya 3100 MC - Client for Nokia and Avaya 3100 MC - Client for Windows Mobile do not contain integrated virtual private network (VPN) software. Any industry-standard VPN software for the Nokia or Windows Mobile device can be used.

The Avaya 3100 MC - Client for Nokia and Avaya 3100 MC - Client for Windows Mobile communicate directly to the Avaya 3100 Mobile Communicator Gateway. When deployed with the BES, the Avaya 3100 MC - Client for BlackBerry communicates with the BES, which communicates with the Avaya 3100 Mobile Communicator Gateway. When deployed without the BES, the Avaya 3100 MC - Client for BlackBerry communicates directly with the Avaya 3100 Mobile Communicator Gateway.

The Avaya 3100 MC - Web UI does not require software installation on the device. When the Avaya 3100 MC - Web UI runs on a BlackBerry that uses a BES, the BlackBerry Web browser uses the Mobile Data Service (MDS) on the BES to access the Avaya 3100 Mobile Communicator Gateway. For the non-BES BlackBerry, and for Windows Mobile and Nokia devices, the Avaya 3100 MC - Web UI (in the Web browser) uses HTTPS to connect to the Avaya 3100 Mobile Communicator Gateway.

For examples of Avaya 3100 MC - Client and Avaya 3100 Mobile Communicator Gateway call flows, see *Avaya 3100 Mobile Communicator Fundamentals*, NN42030-109.

Avaya 3100 Mobile Communicator Gateway network deployment

The Avaya 3100 Mobile Communicator Gateway requires the following network infrastructure:

- access to an Enterprise Call Server (ECS) including a call server, Session Initiation Protocol (SIP) gateway, and SIP Proxy Server (SPS)
- access to the ECS Telephony Local Area Network (TLAN), including all SIP infrastructure, media gateways, and any IP endpoint that can originate or terminate real-time transport
- access to a BlackBerry Enterprise Server (BES) if the Avaya 3100 Mobile Communicator Gateway supports the Avaya 3100 MC - Client for BlackBerry with the BES

[Figure 2: Data access from devices](#) on page 15 shows data access from the devices.

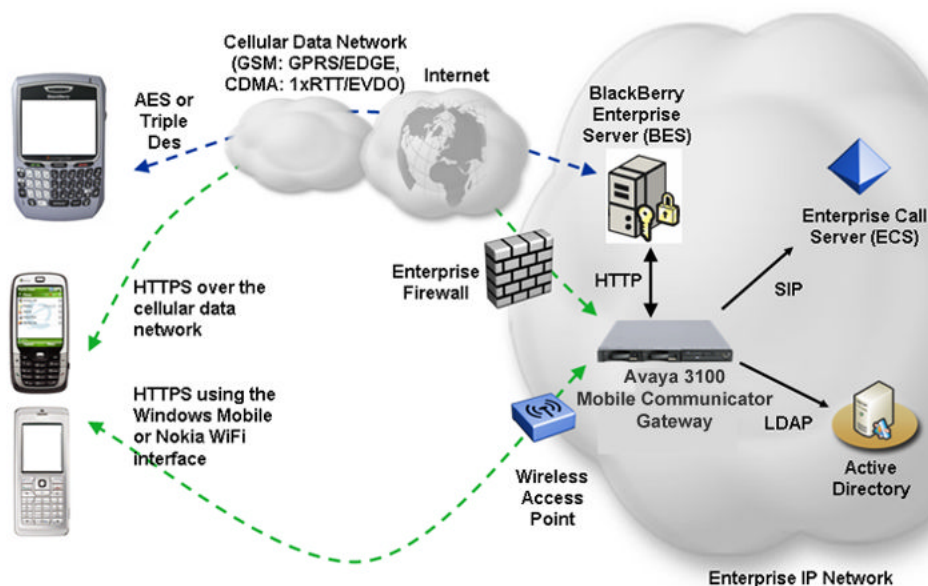


Figure 2: Data access from devices

The Avaya 3100 Mobile Communicator Gateway requires the following network infrastructure with the Avaya CS 1000:

For examples of Avaya 3100 MC - Client and Avaya 3100 Mobile Communicator Gateway call flows, see *Avaya 3100 Mobile Communicator Fundamentals, NN42030-109*.

Communication server requirements

Avaya 3100 Mobile Communicator Release 3.1 supports the following versions of Avaya Communication Server 1000 (Avaya CS 1000):

- Avaya CS 1000 Release 5.5
 - CS and SS: Deplist of February 3, 2009 or later
 - SPS: SU 5.50.12.006 or later
- Avaya CS 1000 Release 6.0
 - latest deplist must be loaded

Avaya CS 1000 package requirements are discussed in [Avaya CS 1000 package requirements](#) on page 30.

Avaya 3100 Mobile Communicator Release 3.1 supports the following versions of Avaya Communication Server 2100 (Avaya CS 1000):

Avaya CS 1000 SE 11

Dialing plans and telephone numbers

Avaya 3100 Mobile Communicator supports telephone numbers in the following formats

- Dial strings, where the user enters all the digits to be dialed. Examples of dial strings include 2356, 63432356, 93432356 and 3432356.
- E.164 Fully Qualified International Numbers, where telephone numbers start with the plus (+) symbol. E.164 Fully Qualified International Numbers are also known as "plus numbers". Examples of Fully Qualified International Numbers include +16131234567 and +31123456789.

On all mobile phones, mobile carriers support the plus (+) sign in telephone numbers. The + identifies that this is an E.164 fully qualified international number (for example, see <http://unifiedcommunicationsblog.globalknowledge.com/2009/07/02/e164-the-modern-dial-plan/>).

If you use the +, you do not need to use an international dial prefix (for example, 011). Avaya 3100 Mobile Communicator supports the same dial plan as the mobile carrier by supporting the +. On devices with a keyboard, the + has its own key (for instance, the 'O' on a BlackBerry). On devices without a QWERTY keyboard, inserting the + is specific to the device.

The dial plan available from Avaya 3100 Mobile Communicator should be the same as the dial plan for a desk telephone. That is, if the user has a desk telephone and an Avaya 3100 MC - Client device, the dial plan should be the same.

Avaya 3100 Mobile Communicator users should use the E.164 Fully Qualified International Numbers for all stored Public Switched Telephone Network (PSTN) numbers in address books and mobile device applications. By using this format, the numbers can be dialed from any region or country, within the wireless network or from the communication server.

The E.164 Fully Qualified International Numbers ensure that users do not need to be concerned about dial prefixes or long distance codes. The network determines how to place the call, based on the user's location and network connection.

When the user dials an E.164 Fully Qualified International Number, the communication server puts the number in the request Uniform Resource Indicator (URI) of the SIP INVITE message in the following format sip: +CCCXXXXXXXX@domain; user=phone.

When using the ECS, configure the CNTC, NATC, and INTC parameters in LD 15 to support E.164 Fully Qualified International Numbers. These parameters ensure that fully qualified numbers within the same country are dialed as national numbers, and international numbers are prefixed correctly.

Example 1 (Switzerland)

ECS is Avaya Communication Server 1000 (Avaya CS 1000) AC1=0, CNTC=41, NATC=0, INTC=00

Call to a number within Switzerland

A user initiates a call to a contact with the phone number +41123456789.

The URI incoming for the SIP INVITE for the call is sip:
+41123456789@domain.com;user=phone

Avaya CS 1000 digit processing strips the CNTC and adds <AC1 + NATC> to produce 00123456789

Call to a number outside Switzerland

A user initiates a call to a contact with the phone number +14161234567.

The URI incoming for the SIP INVITE for the call is sip:
+14161234567@domain.com;user=phone

Avaya CS 1000 digit processing adds <AC1 + INTC> to produce 00014161234567

Example 2 (North America)

ECS is Avaya CS 1000 AC1=6, CNTC=1, NATC=1, INTC=011

Call to a number within North America

A user initiates a call to a contact with the phone number +14161234567.

The URI incoming for the SIP INVITE for the call is sip:
+14161234567@domain.com;user=phone

Avaya CS 1000 digit processing strips the CNTC and adds <AC1 + NATC> to produce 614161234567

Call to a number outside North America

A user initiates a call to a contact with the phone number +41123456789.

The URI incoming for the SIP INVITE for the call is sip:
+41123456789@domain.com;user=phone

Avaya CS 1000 digit processing adds <AC1 + INTC> to produce 601141123456789.

Security requirements

The Avaya 3100 Mobile Communicator Gateway requires data access to the ECS TLAN and uses the ECS SIP Proxy Server (SPS) as the SIP Signaling Proxy. The Avaya 3100 Mobile Communicator Gateway can accept or transmit real time protocol (RTP) messages to any IP endpoint in the Enterprise (for example, Media Cards, other SIP clients, or IP telephones).

[Figure 3: Sample Avaya 3100 Mobile Communicator Gateway firewall configuration](#) on page 19 shows a firewall that separates the Avaya 3100 Mobile Communicator Gateway from the remainder of the Enterprise voice infrastructure. The Avaya 3100 MC - Client for BlackBerry (without the BES), Avaya 3100 MC - Client for Nokia, and Avaya 3100 MC - Client for Windows Mobile require access on the internet to a public FQDN and a public IP address. The figure also shows a sample firewall configuration and policy. For the purposes of this example assume

- that the Avaya 3100 MC - Client (in the absence of a BES) requires a public FQDN and IP for the Avaya 3100 Mobile Communicator Gateway to be accessible from the internet. This in turn forces the Avaya 3100 Mobile Communicator Gateway to be placed in a demilitarized zone (DMZ).
- Firewalls are used to filter traffic from the internet and from the DMZ to separate the Avaya 3100 Mobile Communicator Gateway and internet from the trusted Enterprise voice infrastructure where other components on the ECS TLAN reside.

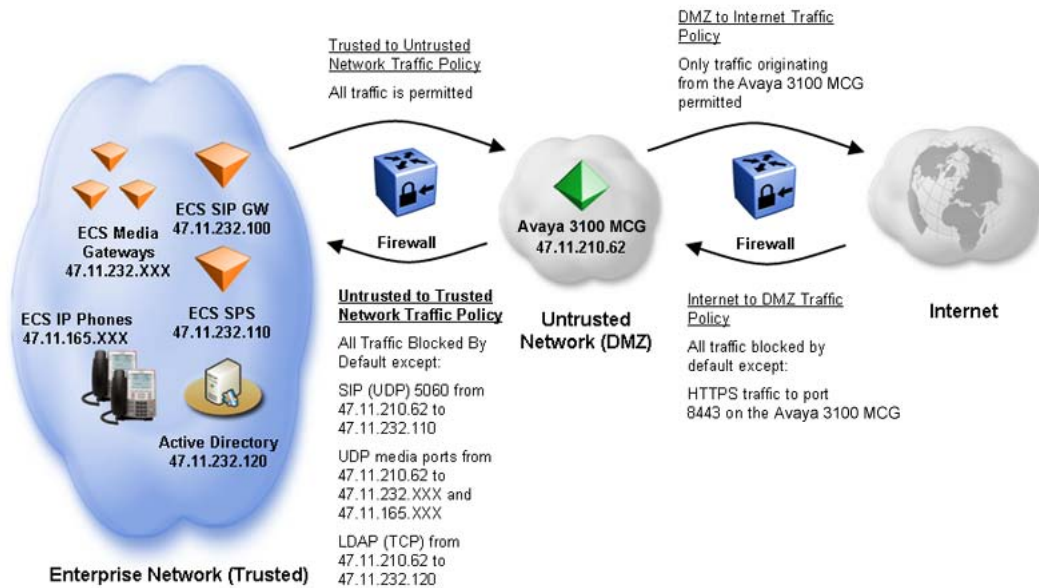


Figure 3: Sample Avaya 3100 Mobile Communicator Gateway firewall configuration

If a user calls a client, the SIP signaling comes through the SPS. Real Time Protocol (RTP) for announcements or Avaya 3100 Mobile Communicator Instant Conference calls takes place between the Avaya 3100 Mobile Communicator Gateway and the IP telephone without using the SPS.

To allow public internet traffic to reach the Avaya 3100 Mobile Communicator Gateway from clients, while simultaneously providing Avaya 3100 Mobile Communicator Gateway access to the ECS TLAN for SIP and RTP, you must carefully consider the data network and security requirements of the Enterprise.

Proprietary communication between the Avaya 3100 Mobile Communicator Gateway and the Avaya 3100 MC - Client for BlackBerry (without the BES, using HTTP), the Avaya 3100 MC - Client for Nokia (using HTTPS), and the Avaya 3100 MC - Client for Windows Mobile (using HTTPS) enables clients to initiate and modify calls for the user on the ECS. In the BES configuration, the Avaya 3100 MC - Client for BlackBerry communicates with the BES, which communicates with the Avaya 3100 Mobile Communicator Gateway. The Avaya 3100 MC - Client for Nokia and Avaya 3100 MC - Client for Windows Mobile communicates directly with the Avaya 3100 Mobile Communicator Gateway, as well as the Avaya 3100 MC - Client for BlackBerry when configured without the BES.

Access to user records in an active directory server configured against the Avaya 3100 Mobile Communicator Gateway uses a tunnel over HTTP or HTTPS. Configure the Avaya 3100 Mobile Communicator Gateway to specify the query search base, which limits the search to a subtree of the base.

The Avaya 3100 Mobile Communicator Gateway queries a corporate Lightweight Directory Access Protocol (LDAP) server when the users use the Directory lookup feature on their clients. The Avaya 3100 Mobile Communicator Gateway supports the following LDAP servers:

- Active Directory/Exchange Server 2000 or 2003
- Avaya Common Network Directory (CND)

High availability

You can deploy the Avaya 3100 Mobile Communicator Gateway as a nonredundant server or in a redundant pair. [Figure 4: Avaya 3100 Mobile Communicator Gateway high availability configuration](#) on page 21 shows the redundant pair configuration that enables the high availability solution.

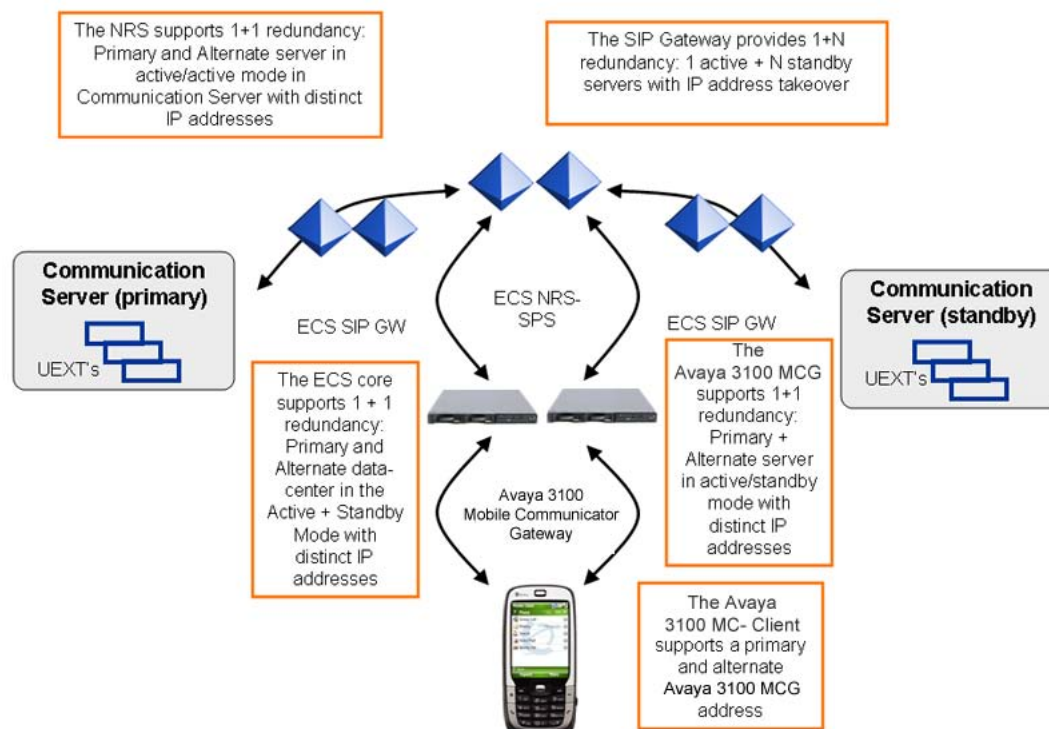


Figure 4: Avaya 3100 Mobile Communicator Gateway high availability configuration

A redundant system includes an active server and a standby server. Mobile clients access the active server, while the standby server functions as a backup. The two roles switch freely, based on the following rules:

- If the Avaya 3100 Mobile Communicator Gateway does not have a configured backup IP address, it starts in active mode.
- If the Avaya 3100 Mobile Communicator Gateway has a configured backup IP address, it starts in inactive mode and attempts to locate the standby system.
 - If the standby server is in standby mode, the system with the lower IP address becomes active.
 - If the standby server is in active mode, the standby server remains active.
 - If the standby server is not located, the local system is declared active.
- If the active system stops, the standby system becomes active.

The pair of Avaya 3100 Mobile Communicator Gateway servers must contain identical software for redundancy to work. Each server acts as the backup for the other server.

The clients support Avaya 3100 Mobile Communicator Gateway redundancy. The Primary Avaya 3100 Mobile Communicator Gateway address and Secondary Avaya 3100 Mobile Communicator Gateway address fields in the clients contain the active and standby Avaya 3100 Mobile Communicator Gateway IP addresses respectively. When the active Avaya 3100

Mobile Communicator Gateway stops responding, the clients switch to the other Avaya 3100 Mobile Communicator Gateway.



Important:

The communication link between two Avaya 3100 Mobile Communicator Gateway servers in the redundant pair must be highly reliable and available. When the gateways cannot communicate with each other, they both become active, start processing traffic, and try to register with the NRS. The NRS has only one gateway endpoint associated with the Avaya 3100 Mobile Communicator Gateway, so the second gateway to register with the NRS receives all the incoming SIP traffic.

Capacity

The Avaya 3100 Mobile Communicator Gateway supports 1500 users per gateway. Avaya testing used a capacity of 8000 calls per hour. The 1500 users per gateway capacity recommendation assumes each user makes on average four calls per hour (or approximately 6000 calls per hour). This results in a margin of safety for the capacity of the Avaya 3100 Mobile Communicator Gateway when servicing 1500 users per gateway.

Chapter 5: Engineering

This chapter details the engineering aspects of the Avaya 3100 Mobile Communicator (Avaya 3100 Mobile Communicator).

Navigation

- [Client device specifications](#) on page 23
- [Gateway specifications](#) on page 23
- [Port tables](#) on page 23

Client device specifications

The Avaya 3100 Mobile Communicator - Client (Avaya 3100 MC - Client) application runs on a number of devices. These devices have no special hardware or software requirements.

To view the list of supported devices, see the Avaya 3100 Mobile Communicator Product Bulletin at <http://www.avaya.com>.

Gateway specifications

The Avaya 3100 Mobile Communicator Gateway uses one of the following servers:

- HP DL320G4
- IBM x306m

The Avaya 3100 Mobile Communicator Gateway runs on the Avaya CS 1000 Linux Base operating system. For more information, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

Port tables

The following table details the ports used in the Avaya 3100 Mobile Communicator Gateway. When using this section to configure firewalls, refer to [Figure 3: Sample Avaya 3100 Mobile Communicator Gateway firewall configuration](#) on page 19.

Table 1: Avaya 3100 Mobile Communicator Gateway ports

Port	Protocol	Function	Applica- tion	Configur- able?	Configure in Avaya 3100 MCG-to-Enterprise Firewall policy?	Configure in Avaya 3100 MCG Firewall policy?
21	Transmissi on Control Protocol (TCP)	File Transfer Protocol (FTP)	Base Linux	No	No	No
22	TCP	Secure Shell (SSH)	Base Linux	No	No	No
53 (Send only)	User Datagram Protocol (UDP)	Domain Name Server (DNS) queries to external DNS server	Base Linux	No	Yes, assuming DNS is within the Enterprise network	No
123 (Send only)	TCP	Network Time Protocol (NTP)	Base Linux	No	Yes, assuming DNS is within the Enterprise network	No
389 (Send only)	LDAP (TCP)	Directory access	Directory access	Yes	Yes	No
1098	TCP	Communicat ion between the Avaya 3100 MCG Administrati on server and the Avaya 3100 Mobile Communicat or Gateway server	Avaya 3100 MCG	No	No	No
1099	TCP	Communicat ion between the Avaya 3100 MCG	Avaya 3100 MCG	No	No	No

Port	Protocol	Function	Applica- tion	Configur- able?	Configure in Avaya 3100 MCG-to-Enterprise Firewall policy?	Configure in Avaya 3100 MCG Firewall policy?
		server and the Avaya 3100 Mobile Communicat or Gateway Administrati on server				
3306	TCP	SQL Client Access	MySQL	No	No	No
5060	Session Initiation Protocol (SIP) (UDP)	Avaya 3100 MCG listen port for Voice over IP (VoIP) Signalling	Avaya 3100 MCG	Yes	Yes	No
5072	SIP (UDP)	Avaya 3100 MCG listen port for VoIP Signalling (Instant Call Server)	Avaya 3100 MCG	Yes	Yes	No
7800	TCP	Avaya 3100 MCG Data Replication	Avaya 3100 MCG	No	No	No
8008	HTTP (TCP)	Licensing validation with www199.nor tel.com	Avaya 3100 MCG	No	No	No
8080	TCP	Avaya 3100 MC - Client open client interface	Avaya 3100 MC - Client	Yes 8080 to 8089	No	Yes
8282	HTTP (TCP)	Avaya 3100 MCG Open Web Admin Interface (standalone	Avaya 3100 MCG Web Administratio n Console	No	No	No

Port	Protocol	Function	Applica- tion	Configur- able?	Configure in Avaya 3100 MCG-to-Enterprise Firewall policy?	Configure in Avaya 3100 MCG Firewall policy?
		managemen t only)				
8443	HTTPS (TCP)	Avaya 3100 MC - Client Secure Client Interface	Avaya 3100 MCG	Yes 8440 to 8449	No	Yes
8553	TCP	Avaya 3100 MCG Secure Admin Interface (standalone managemen t only)	Avaya 3100 MCG Admin	No	No	No
9800	TCP	Avaya 3100 MCG Server Java Virtual Machine (JVM)	Avaya 3100 MCG JVM	No	No	No
9801	TCP	Avaya 3100 MCGAdmini stration JVM	Avaya 3100 MCG Admin JVM	No	No	No
26000 to 26099 (listen only)	UDP	Media for all Avaya 3100 MC - Client calls anchored on the Avaya 3100 MCG	Voice over IP (VoIP) Conference Media	Yes	Yes	No
27000 to 27099 (listen only)	RTP (UDP)	Media for all Avaya 3100 MC - Client calls anchored on the Avaya 3100 MCG	VoIP Media	Yes	Yes	No

In the preceding table, the ranges 26000 to 26999 and 27000 to 27999 depend on the configuration of the Maximum number of DTR ports parameter.

The following table lists the ports that are defined by the Enterprise Call Server (ECS). You configure these ports on the ECS.

Table 2: ECS ports

Protocol	Function	Application	Configure in the Avaya 3100 Mobile Communicator Gateway-to-Enterprise Firewall policy?	Configure in the Internet-to-Avaya 3100 Mobile Communicator Gateway Firewall policy?
RTP (UDP)	VoIP send port for the Gateway server. Configured on the Avaya 3100 MCG.	Avaya 3100 MCG	Yes	No
RTP (UDP)	VoIP send port for the Instant Conference Server. Configured on the Avaya 3100 MCG.	Avaya 3100 MCG	Yes	No
RTP (UDP)	VoIP send port for the VoIP Conference Media. RTP can be sent to media gateways, IP endpoints, or other SIP User Agents. The range of end point ports defines the ports to which the Avaya 3100 MCG sends media.	Avaya 3100 MCG	Yes	No
RTP (UDP)	VoIP send port for Media. RTP can be sent to media gateways, IP endpoints, or other SIP User Agents. The range of end point ports defines the ports to which the Avaya 3100 MCG sends media.	Avaya 3100 MCG	Yes	No

Chapter 6: Interworking requirements with CS 1000

This chapter details the interworking requirements for the Avaya 3100 Mobile Communicator (Avaya 3100 Mobile Communicator) and Avaya Communication Server 1000 (Avaya CS 1000), which is a supported Enterprise Call Server (ECS).

Navigation

- [Avaya CS 1000 deployment considerations](#) on page 29
- [Avaya CS 1000 Source Based Routing](#) on page 29
- [Avaya CS 1000 package requirements](#) on page 30
- [Avaya CS 1000 engineering for Avaya 3100 Mobile Communicator](#) on page 30
- [Avaya CS 1000 capacity requirements](#) on page 37
- [Avaya CS 1000 and supported Avaya 3100 Mobile Communicator features](#) on page 42
- [Call Detail Recording](#) on page 44

Avaya CS 1000 deployment considerations

The Avaya 3100 Mobile Communicator Gateway requires data access to the Avaya CS 1000 Telephony Local Area Network (TLAN). The Avaya 3100 Mobile Communicator Gateway uses the Avaya CS 1000 Session Initiation Protocol (SIP) Proxy Server (SPS) as the SIP Signaling Proxy. The Avaya 3100 Mobile Communicator Gateway accepts or transmits real time protocol (RTP) messages to any IP endpoint within the Enterprise (for example, Media cards, other SIP clients, or IP telephones).

To allow public internet traffic to reach the Avaya 3100 Mobile Communicator Gateway from clients, while simultaneously providing Avaya 3100 Mobile Communicator Gateway access to the Avaya CS 1000 TLAN for SIP and RTP, you must carefully consider the data network and security requirements of the Enterprise.

Avaya CS 1000 Source Based Routing

Avaya CS 1000 Source Based Routing (SBR) occurs when the request Uniform Resource Indicator (URI) of the INVITE message sent from the Avaya 3100 Mobile Communicator

Gateway contains the tag `x-nt-net-feature=x-nt-home`. For example, the following request URI triggers SBR:

```
INVITE sip:+16131234567@avaya.com;x-nt-sip-line-service;x-nt-net-feature=x-nt-home SIP/2.0
```

SBR causes the Avaya CS 1000 Network Routing Service-SIP Proxy Service (NRS-SPS) to route the call attempt (INVITE) to the P-Asserted-Id in the SIP INVITE instead of using the Request URI.

Using SBR means that all calls from a SIP user route to the home call server for origination, allowing the call server to apply features such as Calling Line ID (CLID) and Network Class of Service (NCOS) to SIP calls.

In the Avaya 3100 Mobile Communicator Gateway, use the User Prefix/Phone-context for Call origination field to configure SBR. For information, see *Avaya 3100 Mobile Communicator Administration and Security, NN42030-600*.

Avaya CS 1000 package requirements

Avaya CS 1000 requires the following packages to support Avaya 3100 Mobile Communicator:

- FMCL package (414)
- Mobile Extension (412)
- PCA (398)
- ISDN (145)

If the Avaya 3100 Mobile Communicator supports the CallPilot Message Waiting Indicator, the following package must be licensed:

Premium Service and NMC (175, 219)

Avaya CS 1000 engineering for Avaya 3100 Mobile Communicator

The Avaya 3100 Mobile Communicator - Web UI, Avaya 3100 MC - Client for BlackBerry, Avaya 3100 MC - Client for Nokia, Avaya 3100 MC - Client for Windows Mobile, and Avaya 3100 Mobile Communicator Gateway depend on the following Avaya CS 1000 components:

- Avaya CS 1000

- Each user requires one Universal Extension (UEXT). Each UEXT supports the SIP interface on the client. Configure the UEXT with the Fixed Mobile Convergence Line (FMCL) subtype.

The FMCL subtype requires an Incremental Software Management (ISM) independent of the Mobile Extension (MOBX) subtype.
- SIP Access Port license
- SIP Gateway
- SPS, using the Avaya CS 1000 NRS-SPS on the Linux-based NRS.
 - Configure each Avaya 3100 Mobile Communicator Gateway as a Dynamic Gateway Endpoint with an endpoint name. Configure the Dynamic Gateway Endpoint with authentication turned off.
 - Each client requires the configuration of an NRS-SPS User Endpoint (UE). Clients use the UE for user name and password information, not for SIP routing. Therefore, the NRS-SPS must never match a destination number against the client UEs (including the corresponding UEXT Target DN).
- SPS, using the Avaya CS 1000 Release 6.0 NRS

Avaya 3100 Mobile Communicator Gateway must be configured to use proxy mode when registering to this server.

The Direct Inward Dial (DID) number for the Dial in Service DN terminates on the Avaya 3100 Mobile Communicator Gateway.

Configure the Avaya CS 1000 with a mobility prefix to support the client. The UEXT target DN uses the mobility prefix as a prefix to identify mobile users. The Mobility Prefix is the Local Exchange code (NXX) that directs the call to the Avaya 3100 Mobile Communicator within the desired dialing plan. The Mobility Prefix is a unique digit sequence that does not conflict with the existing Avaya CS 1000 Universal Dialing Plan (UDP), Coordinated Dialing Plan (CDP), and routing configuration.

The Multiple Access Directory Number (MADN) is a DN that appears on multiple terminal numbers (TN). The Multiple Appearance Directory Number Redirection Prime (MARPDN) is a designation that is put on one of the TNs to identify that specific features apply to the DN that is on multiple TNs should be configured for the group on the TN that is the MARPDN. For more information, see *Avaya Communication Server 1000 Features and Services Fundamentals, NN43001-106*.

The Avaya CS 1000 NRS-SPS supports the Source Based Routing (SBR) feature. SBR ensures that, for all users of an Avaya 3100 Mobile Communicator Gateway, the CLID NCOS and dial plan they see on their mobile phone is consistent with their desk phone. The SPS routes all Avaya 3100 Mobile Communicator call attempts to the user's home call server so that those features configured on the home call server can be applied to the Avaya 3100 Mobile Communicator call. For information about Source Based Routing (SBR), see [Avaya CS 1000 Source Based Routing](#) on page 29.

Figure 5: Client with Avaya CS 1000 and UDP on page 32 shows an example of clients using Avaya CS 1000 and UDP.

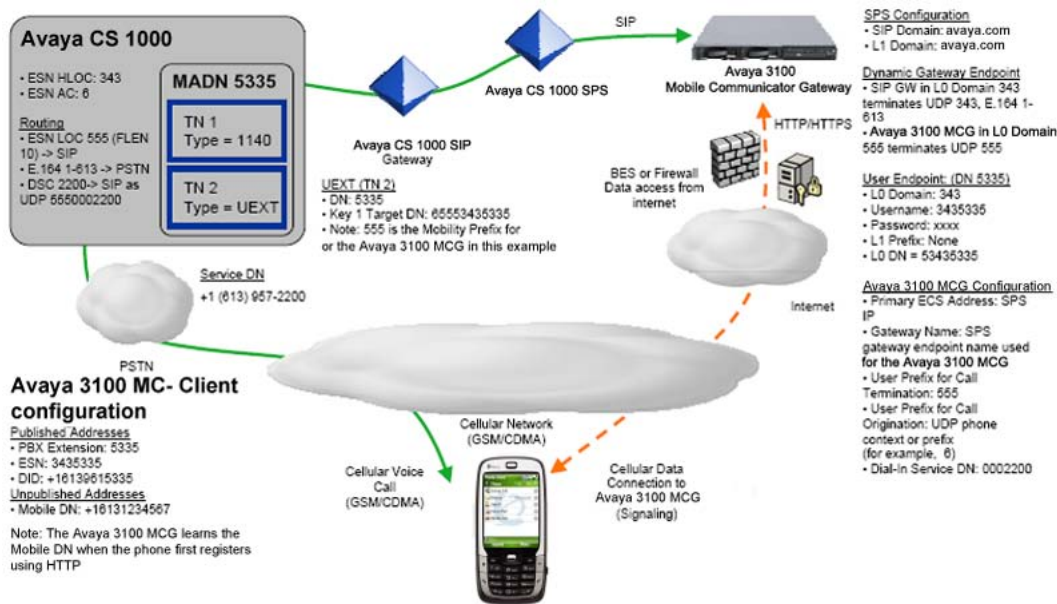


Figure 5: Client with Avaya CS 1000 and UDP

Figure 6: Client with Avaya CS 1000 and CDP on page 32 shows an example of clients using Avaya CS 1000 with CDP.

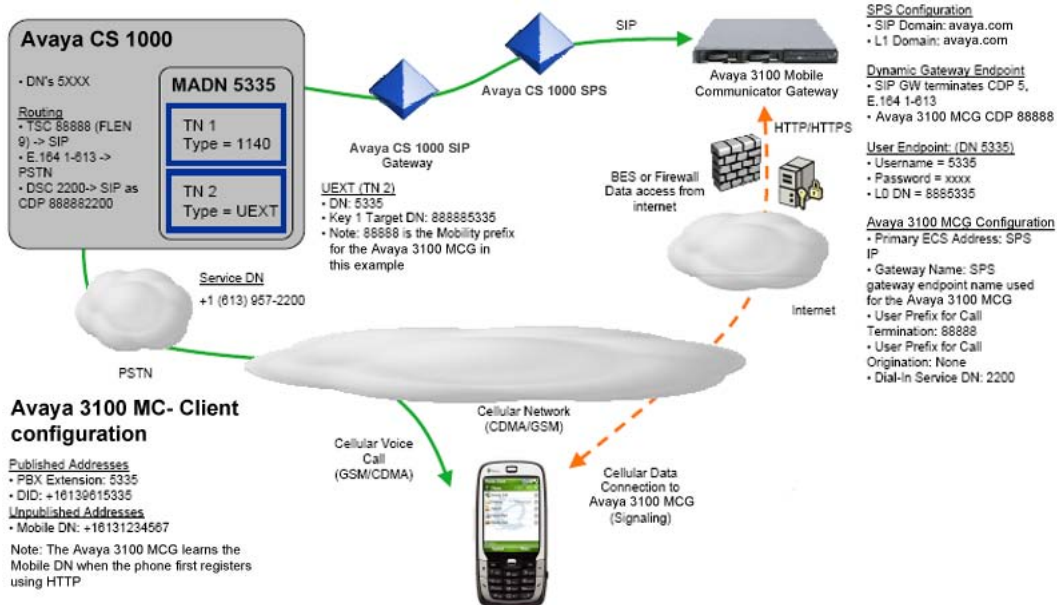


Figure 6: Client with Avaya CS 1000 and CDP

The UEXT configuration requirements are shown in the following table.

Table 3: UEXT configuration parameters

Parameter	Description	UDP example	CDP example
Subtype	UEXT subtype; must be FMCL	FMCL	FMCL
primary DN	On key 0; this determines the user's published addresses for both private electronic switched network (ESN) and public direct inward dial (DID).	5335 contributes to an ESN of 3435335 and a DID of +16139615335	5335 contributes to a DN of 3435335 and a DID of +16139615335
target DN	Extends the user's incoming calls to mobile clients that are accessible through the SIP domain	65553435335 where 555 is the Mobility prefix	888885335 where 88888 is the Mobility prefix

On the NRS-SPS, configure the UE attributes as described in [Table 4: User Endpoint attributes](#) on page 33.

For more information about UEXTs, see *Avaya Communication Server 1000 Features and Services Fundamentals – Book 6 of 6, NN43001-106-B6*.

Table 4: User Endpoint attributes

Parameter	Description	Example
User name	User's Electronic Switched Network (ESN) number	3435335
Tandem gateway endpoint name	Endpoint name. Do not configure this parameter	
L0 DN	Based on the user's directory number (DN). Cannot match anything in the Coordinated Dialing Plan or unqualified dialing plan. This cannot match because the only rule needed on the NRS for routing Avaya 3100 Mobile Communicator calls is the rule setup to route any number with the mobility prefix to the Avaya 3100 Mobile Communicator Gateway. All calls (service DN and UEXT calls) destined for the Avaya 3100 Mobile Communicator Gateway must have the mobility prefix and use that rule. If the user endpoint had a DN that matched something else in the dial plan it would conflict with the mobility prefix routing rule or the basic	53435335

Parameter	Description	Example
	dialplan. Can be the last digit of the mobility prefix with the User's ESN DN.	
L1 DN prefix	not required	
Authentication enabled	Determines if Authentication is required.	Authentication on
Authentication password	The password for authentication	xxxxxxx

For information about SIP Gateway configuration, see *IP Peer Networking Installation and Commissioning, NN43001-313*.

SIP Trunk configuration

You must configure the communication server SIP trunk that receives Avaya 3100 Mobile Communicator Gateway calls, on behalf of mobile client users, to ESN5. You must configure all associated Virtual trunks to WNK/WNK. The mobile client requires these settings so that calls to the Public Network display the correct Calling Line ID (CLID) and have the same Network Class of Service (NCOS) as a call from the associated communication server telephone.

The output for the WNK/WNK Virtual Trunk, from Element Manager or a terminal window, looks like this:

```
DES IPTIE
TN 081 0 00 02 VIRTUAL
TYPE IPTI
CDEN 8D
CUST 0
XTRK VTRK
ZONE 000
TRK ANLG
NCOS 0 RTMB 10 3
CHID 3
TGAR 0
STRI/STRO WNK WNK
SUPN YES
AST NO
IAPG 0 *
CLS UNR DIP WTA LPR APN THFD XREP
P10 NTC MID
TKID *
AACR NO
```



Important:

All of the SIP Virtual Trunks must be configured to WNK WNK.

The output for the ESN5 Route Data Block, from Element Manager or a terminal window, looks like this:

```

TYPE RDB
CUST 00
DMOD
ROUT 10
DES IPROUTE
TKTP TIE

...
VTRK YES
ZONE 100
PCID SIP

...
ANTK
SIGO ESN5
STYP SDAT

```

**Important:**

If the Route Data Block (RDB) already has associated Virtual Trunks and is configured to SIGO STD, you must remove all Virtual Trunks before you can change the RDB to ESN5.

Device Handoff configuration

Device handoff permits the Avaya 3100 Mobile Communicator user to hand off an established call between the mobile phone and the desk telephone. The desk telephone must be configured with a handoff key. Device handoff can be used only when the desk telephone and the Universal Extension (UEXT) share the same primary DN in a Single Call Ringing (SCR) configuration. Device handoff is not supported when the desk telephone and Avaya 3100 MC - Client user are in a Multiple Call Ringing (MCR) arrangement. In this situation, the user must transfer the call between the appearances.

Device handoff requires the configuration of the handoff key on the desktop telephone. Device handoff is supported on any Avaya CS 1000 telephone that supports the configuration of fixed feature keys. These telephones include the Avaya IP Deskphones (with Unified Network IP Stimulus Protocol [UNiStim] firmware), the IP Softphone 2050, and Time Division Multiplex (TDM) telephones.

On the mobile phone, there is no privacy protection if the UEXT does not have Station Control Password (SCPW) configured. For desk telephones (even with SCPW), there is no privacy protection if the desk telephone has Privacy Override Allowed (CLS POA) or if the desk telephone is an analog telephone (500- or 2500-type telephone).

For SCPW privacy protection on the mobile phone, the system administrator must configure the SCPQ length under LD 15 CDB FFC_DATA SCPL, and the SPQ on the UEXT under LD 11 SCPW prompt.

In addition, the following configuration requirements must be met:

- FMCL and Mobile X (MOBX) cannot coexist with same DN.
- the DN can only have one of the following UEXT types: SIP3, SIPN, FMCL.

For more information, see *Avaya 3100 Mobile Communicator and Avaya Communication Server 1000 Solution Integration Guide, NN49000-315* and *Avaya Communication Server 1000 Features and Services Fundamentals, NN43001-106*.

Avaya CS 1000 system redundancy

The clients support a high availability configuration for improved redundancy and failover. Configure the client with primary and secondary proxy addresses that refer to different NRS-SPSSs. The clients use an options heartbeat to determine proxy availability. You can configure the heartbeat time.

The clients also support existing SIP redundancy mechanisms in both communication servers within a SIP deployment.

Call Forward No Answer feature interactions

It can be necessary to increase the Call Forward No Answer (CFNA) timeout for mobile client users. The UEXT extends all calls to the Avaya 3100 Mobile Communicator Gateway. The Avaya 3100 Mobile Communicator Gateway then presents the incoming call to the Avaya 3100 MC - Client over the cellular data channel of the Avaya 3100 MC - Client (using HTTP/HTTPS).

It can take a few seconds for the data transmission to reach the client, depending on the current state of the mobile client. If the CFNA timeout is too short, users do not have reasonable time to (potentially) log on and answer the call before the call server invokes CFNA and sends the call to the CFNA destination.

To increase the CFNA timeout, configure the CS 1000 using LD 15 and LD 11.

LD 15 configures the CFN0, CFN1, and CFN2 indexes:

```
LD 15
REQ: chg
TYPE: rdr
TYPE RDR_DATA
CUST 0
OPT
FNAD
FNAT
FNAL
CFTA
CCFWDN
CFN0
CFN1 6
CFN2
DFN0
DFN1
DFN2
MDID
NDID
```

```

MWFB
TRCL
CRTOD
CRDAY
CRHOL

```

LD 11 configures the number of ringing cycles for CFNA. Configure the CFN index that corresponds to the RCO entry configured in LD 15 (for example, RCO 1 uses CFN 1).

```

LD 11
REQ: chg
TYPE: 1140
TN 100 0 8 23
ECHG yes
ITEM rco 1
ITEM
HNT FNA
HNT FNA

```

Avaya CS 1000 capacity requirements

An Avaya 3100 Mobile Communicator implementation requires the CS 1000 system to include the appropriate number of Public Service Telephone Network (PSTN) connections (for example, Primary Rate Interface [PRI] or digital trunk interface [DTI] trunks), SIP Access Ports, and UEXTs.

Avaya 3100 Mobile Communicator licenses include one SIP Access Port per client license.

For deployments with unusual trunking requirements, the number of SIP Access Ports and PSTN trunks must be calculated as described below.

The number of configured users and the required Centi-Call Seconds (CCS) per User determine the required number of PSTN connections and trunks. The CCS per User represents the amount of time a circuit is occupied by each user in 100 seconds (for example, 6 CCS per user means each user is busy 600 seconds during an hour). Choose the CCS per User value based on the typical call load requirements. A value of 6 CCS per User represents normal users; heavier users have progressively higher values. For example, call center telephones normally have CCS per User values of 33.

You can use one of the two following methods to calculate the PSTN trunks and SIP Access Ports:

- [Trunk calculation: Method 1](#) on page 38
- [Trunk calculation: Method 2](#) on page 39

To calculate the number of UEXTs required, see [UEXT calculations](#) on page 42.

For more information about Avaya CS 1000 capacity, see *Avaya Communication Server 1000E Planning and Engineering*, NN43041-220.

Trunk calculation: Method 1

Follow these steps:

1. Add the number of client users.
2. Locate the resulting number in the Number of Users column in [Table 5: Poisson trunk table](#) on page 38.
3. Select the appropriate PSTN and SIP Access Port parameters based on the required CCS per Users.

[Table 5: Poisson trunk table](#) on page 38 uses a Poisson value of P.01, which represents 1 percent blocking.

Table 5: Poisson trunk table

Number of users	Parameter	Up to 6 CCS per User	Up to 12 CCS per User	Up to 18 CCS per User	Up to 24 CCS per User
6	PSTN	5	6	6	6
	SIP Access Port	10	12	12	12
12	PSTN	7	10	12	12
	SIP Access Port	14	20	24	24
18	PSTN	9	13	18	18
	SIP Access Port	18	26	36	36
24	PSTN	10	16	22	24
	SIP Access Port	20	32	44	48
50	PSTN	17	28	38	48
	SIP Access Port	34	56	76	96
75	PSTN	22	38	53	68
	SIP Access Port	44	76	106	136
100	PSTN	28	48	68	87
	SIP Access Port	56	96	136	174
150	PSTN	38	68	97	125
	SIP Access Port	76	136	194	250
200	PSTN	48	87	125	162
	SIP Access Port	96	174	250	324

Number of users	Parameter	Up to 6 CCS per User	Up to 12 CCS per User	Up to 18 CCS per User	Up to 24 CCS per User
300	PSTN	68	125	180	238
	SIP Access Port	136	250	360	476
400	PSTN	82	162	238	317
	SIP Access Port	164	324	476	634
500	PSTN	106	198	297	396
	SIP Access Port	212	396	594	792
600	PSTN	125	238	356	475
	SIP Access Port	250	476	712	950
700	PSTN	144	277	416	554
	SIP Access Port	288	554	832	1108
800	PSTN	162	317	475	633
	SIP Access Port	324	634	950	1266
900	PSTN	180	356	534	712
	SIP Access Port	360	712	1068	1424
1000	PSTN	198	396	594	792
	SIP Access Port	396	792	1188	1584

Example

In a system with 100 users and 6 CCS per User, use [Table 5: Poisson trunk table](#) on page 38 to locate 100 in the Number of Users column. Use the Up to 6 CCS per User column to find the following parameters:

- PSTN = 28
- SIP Access Port = 56

Trunk calculation: Method 2

Follow these steps:

1. To determine the number of PSTN trunks required, add the number of clients to obtain the total number of users.
2. Multiply the total number of users by the desired CCS per User number to obtain a CCS value.

3. Use [Table 6: Trunk traffic Poisson 1 percent blocking](#) on page 40 to find the CCS value and obtain the number of PSTN trunks (in the cell to the left of the CCS number). If the CCS value is between two values in the trunks column, choose the higher number of trunks. For trunk traffic greater than 6068 CCS, allow 30.34 CCS per trunk.
4. Multiply the number of PSTN trunks by two to obtain the number of SIP Access Ports required.

Table 6: Trunk traffic Poisson 1 percent blocking

Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS
1	0.4	51	1291	101	2847	151	4460
2	5.4	52	1322	102	2879	152	4492
3	15.7	53	1352	103	2910	153	4525
4	29.6	54	1382	104	2942	154	4557
5	46.1	55	1412	105	2974	155	4590
6	64	56	1443	106	3006	156	4622
7	84	57	1473	107	3038	157	4655
8	105	58	1504	108	3070	158	4686
9	126	59	1534	109	3102	159	4721
10	149	60	1565	110	3135	160	4754
11	172	61	1595	111	3166	161	4786
12	195	62	1626	112	3198	162	4819
13	220	63	1657	113	3230	163	4851
14	244	64	1687	114	3262	164	4884
15	269	65	1718	115	3294	165	4917
16	294	66	1749	116	3326	166	4549
17	320	67	1780	117	3359	167	4982
18	346	68	1811	118	3391	168	5015
19	373	69	1842	119	3424	169	5048
20	399	70	1873	120	3456	170	5081
21	426	71	1904	121	3488	171	5114
22	453	72	1935	122	3520	172	5146
23	480	73	1966	123	3552	173	5179
24	507	74	1997	124	3594	174	5212

Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS
25	535	75	2028	125	3616	175	5245
26	562	76	2059	126	3648	176	5277
27	590	77	2091	127	3681	177	5310
28	618	78	2122	128	3713	178	5343
29	647	79	2153	129	3746	179	5376
30	675	80	2184	130	3778	180	5409
31	703	81	2215	131	3810	181	5442
32	732	82	2247	132	3843	182	5475
33	760	83	2278	133	3875	183	5508
34	789	84	2310	134	3907	184	5541
35	818	85	2341	135	3939	185	5574
36	847	86	2373	136	3972	186	5606
37	876	87	2404	137	4004	187	5639
38	905	88	2436	138	4037	188	5672
39	935	89	2467	139	4070	189	5705
40	964	90	2499	140	4102	19	5738
41	993	91	2530	141	4134	191	5771
42	1023	92	2563	142	4167	192	5804
43	1052	93	2594	143	4199	193	5837
44	1082	94	2625	144	4231	194	5871
45	1112	95	2657	145	4264	195	5904
46	1142	96	2689	146	4297	196	5937
47	1171	97	2721	147	4329	197	5969
48	1201	98	2752	148	4362	198	6002
49	1231	99	2784	149	4395	199	6035
50	1261	100	2816	150	4427	200	6068

Example

In a system with 100 users and 6 CCS per User, the number of CCS required is 600 (100 users multiplied by 6 CCS per User). Locate 600 CCS in [Table 6: Trunk traffic Poisson 1 percent blocking](#) on page 40.

The entry in the table shows the number of PSTN trunks is between 27 and 28 (between 590 and 618 CCS). Therefore, choose 28 as the number of PSTN trunks.

The number of SIP Access Ports is the number of PSTN trunks multiplied by 2, which is $28 \times 2 = 56$.

UEXT calculations

You require one UEXT for each Avaya 3100 MC - Client user.

Avaya CS 1000 and supported Avaya 3100 Mobile Communicator features

The following table describes the Avaya 3100 Mobile Communicator call features.

Table 7: Avaya 3100 Mobile Communicator call features

	Avaya CS 1000 Mobile Extension	Avaya 3100 MC - Web UI	Avaya 3100 MC - Client
Single Enterprise Number Identity (CDP, UDP, DID)	√	√	√
Enterprise CLID for Outbound Calls from Mobile	√	√	√
Access to Enterprise Dial Plan from Cellular Network	√	√	√
Enterprise Calling Restrictions (NCOS)	√	√	√
Call Forward Support on Call Server (CFB, CFIC, hunting)	√	√	√
Ring Again (against mobile)	√	√	√
Busy Lamp Indication on Attendant Console	√	√	√
Call Detail Recording (CDR)	√	√	√
Busy State (Active Call on Mobile appears on other line appearances and OCS presence as "on the phone" for mobile calls)	√	√	√
Device Handoff—Move active call from mobile to desk phone - Move active call from desk phone to mobile	√	√	√
Single Enterprise Voicemail Mailbox	√	√	√
Enterprise Voicemail Enforcement	√	√	√
Music On Hold	√	√	√

	Avaya CS 1000 Mobile Extension	Avaya 3100 MC - Web UI	Avaya 3100 MC - Client
Support for any phone (mobile, home phone, other)	√	√	Requires installed client
Mid Call Features—Hold, Retrieve, Consultation Call, Transfer, Conference	Using DTMF	Using DTMF	√
Client User Interface For Mobile Features	X	√	√
Enterprise Voicemail MWI	Using third-party application	√	√
Advanced Call Control—Direct Outbound calls from mobile via the enterprise voice network	Carrier support required	X	√
Native Call Intercept—Send calls made from any application on the mobile via the enterprise voice network	NA	X	√
Advanced Call Control—Call Me First calls via the enterprise voice network	X	√	√
Advanced Call Control—Dynamically redirect incoming calls to any phone number	X	X	√
Advanced Call Control—User configurable time of day call routing for inbound calls	X	√	X
Support for Multiple SIM cards	X	√	√
Corporate Directory Search	X	√	√
Presence/IM Support	X	X	√
Enterprise Call Logs	X	X	√
Instant Conferencing (Invite a list of participants defined using a user interface on the client)	X	X	√
Access to Local Directory on Mobile	NA	X	√
Configurable Emergency Number Support via Cellular network	NA	X	√
Customizable voice prompts	NA	NA	√
Integrated with Avaya CS 1000—No additional hardware required	√	COTS platform required	COTS platform required

Call Detail Recording

The mobile clients support Call Detail Recording (CDR) for all calls initiated or accepted by the mobile clients.

Interpret the CDR records according to the type of call made or received by the mobile clients.

Direct outbound call

When a user makes an outgoing call, the mobile client user's home Avaya CS 1000 generates two CDR records.

- The first CDR record provides details of the call from the mobile phone to the service DN. In this record, the originator is the mobile phone number and destination is the service DN.
- The second CDR record provides details of the outgoing call to the called party. In this record, the originator is the username of the mobile client user and the destination is the destination number dialed by the user.

Call-Me-First outbound call

When the user makes a Call-Me-First outbound call, the mobile client user's home Avaya CS 1000 generates two CDR records.

- The first CDR record provides details of the call from the Avaya 3100 Mobile Communicator Gateway to the mobile phone. In this record, the originator is the username of the mobile client and the destination number is the mobile phone number.
- The second CDR record provides details of the outgoing call from the Avaya 3100 Mobile Communicator Gateway to the called party. In this record, the originator is the username of the mobile client user and the destination is the destination number dialed by the user.

Incoming call

For incoming calls, the Universal Extension (UEXT) on the home CS 1000 extends incoming calls to the Avaya 3100 Mobile Communicator Gateway (and eventually to the mobile client). For each incoming call, the UEXT merges two calls: the incoming call to the DN on the Avaya CS 1000 , and then the outgoing extended call to the mobile phone. Incoming calls to the

mobile client that the user answers on the mobile phone generate four CDR records on the home Avaya CS 1000 .

- The first CDR record provides details of the incoming call to the Multiple Appearance DN (MADN). In this record, the originator is the caller and destination is the multiple appearance DN where the UEXT is configured.
- The second CDR record provides the details of the UEXT extended call to the Avaya 3100 Mobile Communicator Gateway (the target DN of the UEXT). In this record, the originator is the MADN number of the UEXT, and the destination is the UEXT target DN that is extending the call to the Avaya 3100 Mobile Communicator Gateway.
- The third CDR record (generated after the UEXT merges the calls) provides details of the originating and terminating parties in the call.
- The fourth CDR record (generated after the user elects to answer the call on their mobile phone) provides the details of the outgoing call from the Avaya 3100 Mobile Communicator Gateway to the mobile phone. In this record, the originator is the username of the mobile client, and the destination is the mobile number of the mobile client user.

Chapter 7: Deployment planning

This section describes the planning required to deploy the Avaya 3100 Mobile Communicator with the Enterprise Call Server (ECS).

For information about the planning aspects related to the Avaya 3100 Mobile Communicator and ECS, see [Planning](#) on page 13 and [Engineering](#) on page 23, which cover the following topics:

- Avaya 3100 Mobile Communicator - Client (Avaya 3100 MC - Client) deployment considerations
- Dialing plans and telephone numbers
- Avaya 3100 Mobile Communicator high availability support
- Avaya 3100 Mobile Communicator port tables
- Avaya CS 1000 deployment considerations

Navigation

- [Licensing requirements](#) on page 48
- [Avaya 3100 MC - Client and Avaya 3100 MC - Web UI licenses](#) on page 48
- [Avaya CS 1000 SIP Gateway CLID Parameters configuration](#) on page 49
- [Mobility prefix](#) on page 52
- [Data access planning](#) on page 53
- [Service DN](#) on page 53
- [Universal Extensions](#) on page 54
- [Caller ID table](#) on page 54

Licensing requirements

Avaya Communication Server 1000 licensing requirements:

- Requires the Avaya Communication Server 1000 Release and corresponding Linux Based NRS
- Uses SIP Access Port Licenses for Avaya CS 1000 SIP infrastructure support
- Avaya CS 1000 requires 1 Universal Extension (UEXT) for each Avaya 3100 MC - Client user. The UEXT is configured with the Fixed Mobile Convergence Line (FMCL) subtype.

Avaya Communication Server 2100 licensing requirements:

- Requires Avaya Communication Server 2100 Release SE 11
- Uses SIP Access Port Licenses for Avaya CS 1000 SIP infrastructure support

Avaya 3100 MC - Client licensing requirements

- Each Avaya 3100 MC - Client requires a license.
- Each license key can only be used once per user.
- The Avaya 3100 MC - Client licenses are installed on the Avaya 3100 Mobile Communicator Gateway.

The Avaya 3100 Mobile Communicator Gateway allocates the license on a first come, first served basis as the Avaya 3100 MC - Client registers with the Avaya 3100 Mobile Communicator Gateway.

- There is no requirement to distribute licenses to each end user.
- The Avaya 3100 Mobile Communicator Gateway administrator can revoke licenses on a per user basis, if necessary, to reclaim user licenses.

Avaya 3100 MC - Client and Avaya 3100 MC - Web UI licenses

The clients and Avaya 3100 MC - Web UI require the following licenses:

- On the Enterprise Call Server (ECS)
 - a SIP Access Port License (on the Signaling Server) for SIP infrastructure support
 - one Universal Extension (UEXT) for each client
- One client license key for each user

The clients require the following licenses with the Avaya CS 1000:

The Avaya 3100 Mobile Communicator Gateway manages the client license keys using site licenses. For more information about Avaya 3100 Mobile Communicator Gateway licensing, see [Avaya 3100 Mobile Communicator Gateway licenses](#) on page 49.

A device which connects using the Avaya 3100 MC - Client or the Avaya 3100 MC - Web UI only consumes one license. The user cannot be connected through the Avaya 3100 MC - Client and the Avaya 3100 MC - Web UI at the same time. Logging in on one interface forces the other interface to terminate.

Avaya 3100 Mobile Communicator Gateway licenses

The Avaya 3100 Mobile Communicator Gateway requires a site license that contains the individual license keys for each client user. The Avaya 3100 Mobile Communicator Gateway allocates the license keys, upon request, to the client.

On the Avaya CS 1000, the Avaya 3100 Mobile Communicator Gateway uses one SIP Access Port license on the Signaling Server. Each client requires one UEXT.

The Avaya 3100 Mobile Communicator Gateway requires internet access to www199.nortel.com (using port 8008) to validate the client licenses on the clients.

During installation, the Avaya 3100 Mobile Communicator Gateway stores the site license file. The site license contains the licenses for the clients. The Avaya 3100 Mobile Communicator Gateway does not distribute the licenses to the clients.

When a user accesses the client application, the client software contacts the Avaya 3100 Mobile Communicator Gateway. The Avaya 3100 Mobile Communicator Gateway allocates licenses on demand until the maximum number of licenses are allocated. The license returns to the pool when the user logs off the client.

The Avaya 3100 Mobile Communicator Gateway administrator can revoke licenses from individual users to reclaim the licenses.

Avaya CS 1000 SIP Gateway CLID Parameters configuration

The SIP Gateway CLID parameters are used to adjust the format of telephone numbers for incoming call appearances. For Avaya 3100 Mobile Communicator, these settings impact the format of numbers that appear on the incoming call popup on the Avaya 3100 MC - Client 3100 client.

Deployment planning

Managing: 192.167.106.3
System » IP Network » Node Configuration » IP Telephony: Node ID 9 » Edit

Edit

Save and Transfer Cancel

- + IP Telephony Node
- + VGW and IP phone codec profile
- + QoS
- + LAN configuration
- + Sntp
- + Virtual Trunk Network Health Monitor configuration
- + H323 GW Settings
- + Firmware
- SIP GW Settings
- TLS Security

Security Policy: Security Disabled

TLS Security Port: 5061 (1 - 65535)

Client Authentication: ☐

Re-negotiation: ☐

X.509 Certificate Authentication: ☐

Primary Proxy or Re-direct Server

Primary Proxy or Redirect (TLAN) IP address: 192.167.107.9

Port: 5060

Supports Registration: ☒

Primary CDS Proxy or Re-direct server flag: ☒

Transport Protocol: UDP

Secondary Proxy or Re-direct Server

Secondary Proxy or Redirect (TLAN) IP address: 0.0.0.0

Port: 5060

Supports Registration: ☐

Secondary CDS Proxy or Re-direct server flag: ☐

Transport Protocol: TCP

CLID Parameters

Country Code (CCC): 1

Area Code (AreaCode): 506 Note: The NPA in North America

Digits to Strip: 0

Prefix to Insert:

Format of CLID: +<CCC><AreaCode><SN>

Subscriber Number (SN):

National Number (NN): 0

International number: +<CCC><NN>

+<International number>

- + SIP URI Map
- + SIP CD Services
- + SIP CTI Services
- + Microsoft Unified Messaging
- + Cards Add
- + Signaling Servers Add

Save and Transfer Cancel

* Mandatory fields of current configuration
Copyright © 2002-2010 Nortel Networks. All rights reserved.

Figure 7: SIP GW CLID Parameters

For all public calls (subscriber [for example, NXX in North America], national [for example, NPA in North America], or international) E.164 fully qualified numbers are used to represent the caller. This is made possible through the use of the following parameters:

- Country Code
- Area Code

- Subscriber/Number of Digits to strip
- Subscriber/Prefix to insert
- National/Number of Digits to strip
- National/Prefix to insert

The E.164 format of subscriber calls (for example, NXX in North America) is:

+<countrycode><area code><subscriber number>.

The parameters Subscriber/Number of digits to strip and prefix to insert are used to modify the format of subscriber numbers presented from the PSTN due to region specific requirements.

The E.164 format of national calls (for example, NPA in North America) is:

+<countrycode><national number>.

The parameters National/Number of digits to strip and prefix to insert are used to modify the format of national numbers presented from the PSTN due to region specific requirements.

Parameter: Country Code

This parameter defines the country code to be used in CLID generation.

Parameter: Area Code

This parameter defines the area code to be used in CLID generation.

Parameter: Subscriber/Number of Digits to strip

For incoming subscriber (NXX) calls this parameter defines the number of digits to strip from the incoming phone number prior to conversion to E.164 format.

Parameter: Subscriber/Prefix to insert

For incoming subscriber (NXX) calls this parameter defines the prefix to insert after stripping any digits necessary from the incoming phone number prior to conversion to E.164 format.

Parameter: National/Number of Digits to strip

For incoming national (NPA) calls this parameter defines the number of digits to strip from the incoming phone number prior to conversion to E.164 format.

Parameter: National / Prefix to insert

For incoming national (NPA) calls this parameter defines the prefix to insert after stripping any digits necessary from the incoming phone number prior to conversion to E.164 format.

Mobility prefix

Before configuring and deploying the Avaya 3100 Mobile Communicator solution, the administrator determines the mobility prefix for the Avaya 3100 Mobile Communicator Gateway. The mobility prefix is a digit prefix used to prefix to all calls that will be sent to the Avaya 3100 Mobile Communicator Gateway. This includes the target DN number of all UEXTs for Avaya 3100 Mobile Communicator users as well as the service DN calls from Avaya 3100 MC - Client clients. The mobility prefix provides a unique digit sequence within the SIP domain to route calls to a specific Avaya 3100 Mobile Communicator Gateway that does not conflict with the existing dial plan and routing configuration for CDP and UDP numbers. If the UEXT target DN did not have this prefix to distinguish Avaya 3100 MC - Client calls, the UEXT extended SIP calls would loop back to the UEXT.

Mobility prefixes have the following requirements:

- One mobility prefix is required per gateway.
- On the call server you must configure
 - The dial plan to send all calls with this prefix to the NRS.
 - All UEXT's for Avaya 3100 MC - Client users must have a target DN with the prefix of the Avaya 3100 Mobile Communicator Gateway to which their Avaya 3100 MC - Client is registered.
 - The incoming service DN call must have its digits manipulated so that the PSTN number dialed for the service DN is mapped to a number prefixed by the mobility prefix. This mapping will trigger the NRS to send this call to the Avaya 3100 Mobile Communicator Gateway3100 and the Avaya 3100 Mobile Communicator Gateway will strip this prefix as with any other mobility prefix prefixed call to reveal the service DN configured on the Avaya 3100 Mobile Communicator Gateway.
- The NRS must have a routing rule to send all calls with this prefix to the Avaya 3100 Mobile Communicator Gateway.
- The mobility prefix is configured on the Avaya 3100 Mobile Communicator Gateway in the User Prefix for Call Termination field.

Data access planning

This section describes things to consider when planning data access.

[Avaya CS 1000 data access considerations](#) on page 53

Avaya CS 1000 data access considerations

The Avaya 3100 Mobile Communicator Gateway requires data access to the TLAN of the Avaya CS 1000. The Avaya 3100 Mobile Communicator Gateway uses the Avaya CS 1000 SPS as the SIP Signaling Proxy. The media for all calls to and from Avaya 3100 MC - Clients is anchored on the Avaya 3100 Mobile Communicator Gateway. The Avaya 3100 Mobile Communicator Gateway will accept or transmit RTP to any IP endpoint within the enterprise (for example, Media Cards, Other SIP clients, IP sets).

Example

If an UNISTIM set calls a user answering through the Avaya 3100 MC - Client on the mobile phone the RTP for the active call will be between the Avaya 3100 Mobile Communicator Gateway and IP set directly and then forwarded from the Avaya 3100 Mobile Communicator Gateway to the Avaya CS 1000 media gateway (for the trunk call to the mobile phone)

Careful consideration is required based on the data network and security requirements of the Enterprise to allow the public internet traffic to reach the Avaya 3100 Mobile Communicator Gateway from the clients while at the same time giving the Avaya 3100 Mobile Communicator Gateway access to the TLAN of the Avaya CS 1000 for SIP and RTP.

Service DN

The Service DN is a PSTN DID DN that is downloaded to the Mobile Client from the Avaya 3100 Mobile Communicator Gateway when it registers to the Avaya 3100 Mobile Communicator Gateway for the first time. When the Mobile Client originates a direct outbound call it dials the Service DN and is connected to the Avaya CS 1000. The Avaya CS 1000 is configured to translate the Service DN to the format <mobility prefix><service DN>. The Avaya CS 1000 then maps the call to the SPS/NRS for resolution. The SPS/NRS then maps the call to the Avaya 3100 Mobile Communicator Gateway based on the routing rule built to resolve all dialing strings preceded by the mobility prefix.

In the following example, 888 is the mobility prefix and 5066404681 is the service Directory Number (DN).

Example: sip:8885066404681@avaya.com

Configure the mobility prefix on the Avaya 3100 Mobile Communicator Gateway configuration tab as the incoming prefix for call termination. Configure the Service DN field on the Avaya 3100 Mobile Communicator Gateway configuration with the service DN.

Universal Extensions

An Avaya CS 1000 Universal Extension (UEXT) represents each mobile client instance.

The Primary DN of the UEXT determines the user's published addresses: both private electronic serial number (ESN) and public direct inward dialing DID (for example, Primary DN: 4680 contributes to the ESN address 8474680 and DID address +15066404680).

The mobility prefix is a prefix to all mobile user identities on the UEXT target DN. The mobility prefix provides a digit sequence that is unique within the SIP domain to identify a mobile client that does not conflict with the existing dial plan and routing configuration for their CDP and UDP numbers.

The Target DN of the UEXT extends the user's incoming calls to mobile clients that are accessible through SIP domain. A typical setup would be AC1 + (mobility prefix) + the user's ESN number (for example, Target DN: 65553435335).



Important:

It can be necessary to increase the Forward No Answer (FNA) timeout for mobile client users. The UEXT extends all calls to the Avaya 3100 Mobile Communicator Gateway. The Avaya 3100 Mobile Communicator Gateway then presents the incoming call to the Avaya 3100 MC - Client clients over the cellular data channel of the Avaya 3100 MC - Client (using HTTP or HTTPS).

It can take a few seconds for the data transmission to reach the client depending on the current state of the mobile phone. If the FNA timeout is too short users do not have reasonable time to (potentially log on) and answer the call before the call server invokes FNA and sends the call to the FNA destination.

Caller ID table

All Avaya CS 1000 telephones use the Caller ID table. The Caller ID table is required for the Avaya 3100 MC - Client to correctly build the Caller ID (CLID) for both Private network and Public network calls from a number or extension.

Outgoing SIP calls from the Avaya 3100 Mobile Communicator Gateway on behalf of the mobile client use the CLID table configured against the Multiple Appearance Directory Number

Redirection Prime (MARP) TN in the Multiple Access Directory Number (MADN) group of the Avaya 3100 MC - Client user.

Chapter 8: Deployment work flow

This section describes the order in which to install the Avaya 3100 Mobile Communicator system and then to interwork the Avaya 3100 Mobile Communicator with the Avaya Communication Server 1000 (Avaya CS 1000).

Deploying the systems task flow

Deploying the systems requires the following procedures.

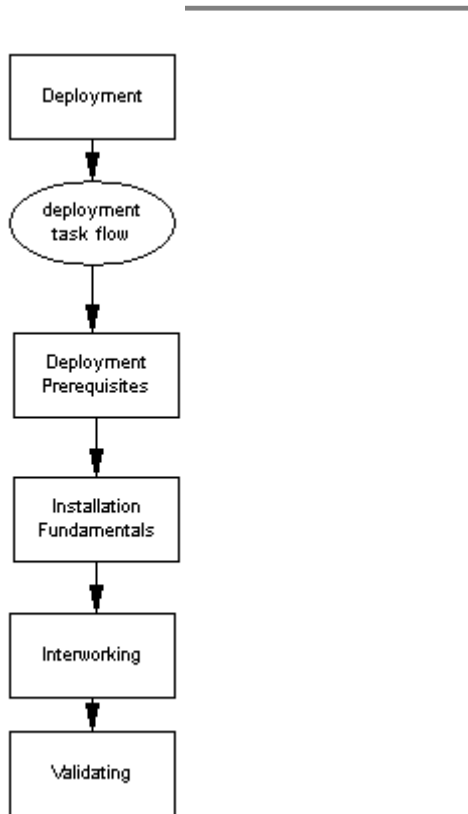


Figure 8: Deploying the system task flow

Task flow navigation

- [Deployment prerequisites](#) on page 59

- [Avaya 3100 Mobile Communicator Gateway installation](#) on page 63
 - [Solution commissioning](#) on page 92
 - [Validate deployment](#) on page 129
-

Chapter 9: Deployment prerequisites

This section describes the prerequisites for Avaya 3100 Mobile Communicator and Avaya Communication Server 1000 (Avaya CS 1000) integration.

- [Establishing the Avaya CS 1000 and Avaya 3100 Mobile Communicator system baseline](#) on page 59
- [Checking the Avaya CS 1000 release from Element Manager](#) on page 61
- [Checking the Avaya CS 1000 release from the command line](#) on page 62

Establishing the Avaya CS 1000 and Avaya 3100 Mobile Communicator system baseline

To successfully integrate voice services, you must first establish the system baseline for the Avaya CS 1000 and Avaya 3100 Mobile Communicator systems so that the systems are configured and working in a stand-alone environment. Use the following table to complete system baselines before integration.

Task	Reference	Comments
Avaya CS 1000		
The Network Numbering Plan is implemented.	<i>Dialing Plans: Description, NN43001-283</i>	Are you using a Unified Dialing Plan (UDP) or a Coordinated Dialing Plan (CDP), or both?
Avaya CS 1000 software is Release 5.5. or higher		To check the release level, see Checking the Avaya CS 1000 release from Element Manager on page 61 or Checking the Avaya CS 1000 release from the command line on page 62.
Basic installation, setup, and configuration of the Call Server components are complete.	<i>Avaya Communication Server 1000M and Meridian 1: Large System Installation and Commissioning, NN43021-310 Avaya Communication Server 1000S: Installation and</i>	

Task	Reference	Comments
	<i>Configuration, 553-3031-210 Avaya Communication Server 1000E: Installation and Commissioning, NN43041-310</i>	
The CS 1000 must have the latest DEP List loaded.	<i>Avaya 3100 Mobile Communicator Release Notes, NN42030-404 (Updates through Product Bulletins)</i>	
The following Avaya CS 1000 packages are required: • FMCL (414) to allow the FMCL UEXTs for Avaya 3100 Mobile Communicator • Mobile Extension (412) to support the UEXT • PCA to configure UEXT sets for mobile users • ISDN (145) to configure ISDN routes when ISDN trunks are used ISMs are required for SIP access ports and FMCL UEXTs. If Call Pilot Message Waiting Indication is required, the Premium Service and NMS packages (175 and 219) are required.		
NRS SIP Proxy Server (SPS)		
NRS SPS software is Avaya CS 1000 Release 5.5.12.006 or higher.		
SPS must have the latest SU loaded	<i>Avaya 3100 Mobile Communicator Release Notes, NN42030-404 (Updates through Product Bulletins)</i>	
Avaya 3100 Mobile Communicator		

Task	Reference	Comments
Avaya 3100 Mobile Communicator is Release 3.1.		
If using BlackBerry devices and the BlackBerry Enterprise Server (BES), the devices and BES must have the BlackBerry Mobile Data Service (MDS) enabled and the devices must be able to access the Fully Qualified Domain Name (FQDN) or IP address of the Avaya 3100 Mobile Communicator Gateway.		
If using mobile devices from the cellular data network (no BES), the Avaya 3100 Mobile Communicator Gateway requires an internet-accessible FQDN and IP address.		
Avaya 3100 Mobile Communicator Gateway must be able to access the Avaya CS 1000 TLAN through the firewall.		
Avaya 3100 Mobile Communicator Gateway license file available		

Checking the Avaya CS 1000 release from Element Manager

Use this procedure to check the version of the CS 1000 using Element Manager.

-
1. Log on to Element Manager.
 2. On the left navigation pane, select Home.
The Home System View page appears.
 3. In the Call Server section, the software release is referred to as Release.
-

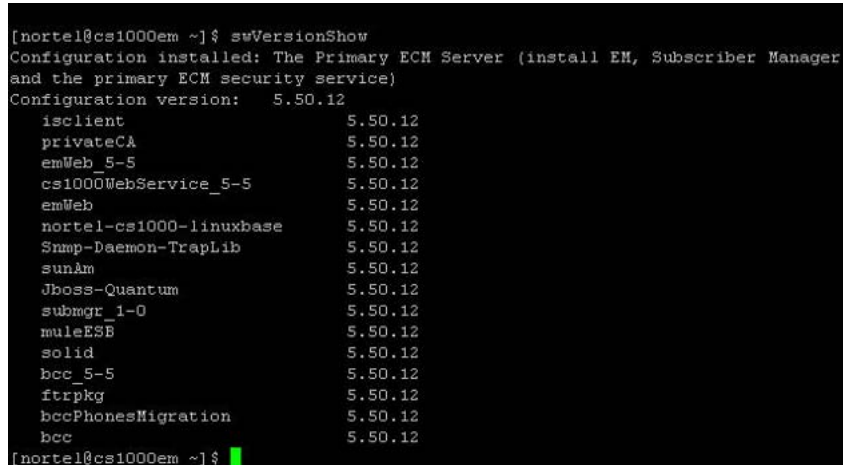
Checking the Avaya CS 1000 release from the command line

Use this procedure to check the version of the CS 1000 using the command line.

1. Log in to the Signaling server or the Enterprise Common Manager server using the **nortel** account.
2. Enter the following command

swVersionShow

The installed software applications and version numbers are displayed. For an example, see the following figure.



```
[nortel@cs1000em ~]$ swVersionShow
Configuration installed: The Primary ECM Server (install EM, Subscriber Manager
and the primary ECM security service)
Configuration version: 5.50.12
  isclient      5.50.12
  privateCA     5.50.12
  emWeb 5-5     5.50.12
  cs1000WebService_5-5 5.50.12
  emWeb        5.50.12
  nortel-cs1000-linuxbase 5.50.12
  Snmp-Daemon-TrapLib 5.50.12
  sunAm        5.50.12
  Jboss-Quantum 5.50.12
  submgr 1-0    5.50.12
  muleESB      5.50.12
  solid        5.50.12
  bcc 5-5      5.50.12
  ftrpkg       5.50.12
  bccPhonesMigration 5.50.12
  bcc          5.50.12
[nortel@cs1000em ~]$
```

Figure 9: swVersionShow example

Chapter 10: Avaya 3100 Mobile Communicator Gateway installation

This chapter contains the instructions for installing a new Mobile Communications Gateway 3100. For information about the Avaya 3100 Mobile Communicator - Client (Avaya 3100 MC - Client) installation, see *Avaya 3100 Mobile Communicator Administration and Security, NN42030-600*.

Important:

Use the server system console for installations and upgrades. Do not use a remote terminal.

Prerequisites to Avaya 3100 Mobile Communicator Gateway installation workflow

- Planning and engineering must be completed as discussed in [Planning](#) on page 13 and [Engineering](#) on page 23.
- Obtain a copy of *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

Avaya 3100 Mobile Communicator Gateway installation workflow

[Figure 10: Installation workflow](#) on page 64 shows the steps required to install the Avaya 3100 Mobile Communicator Gateway. After completing the installation workflow, you configure the system security, configure the client services, install the clients, and back up the Avaya 3100 Mobile Communicator Gateway database. For more information, see *Avaya 3100 Mobile Communicator Administration and Security, NN42030-600*. After configuring the Avaya 3100 Mobile Communicator Gateway, you configure the Avaya 3100 Mobile Communicator to interwork with the appropriate communication server, using the appropriate Solution Integration Guide.

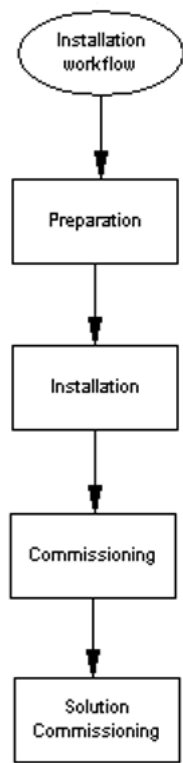


Figure 10: Installation workflow

Result

Workflow navigation

- [Preparation](#) on page 65
- [Installation](#) on page 72
- [Commissioning](#) on page 74
- [Solution commissioning](#) on page 92

[Table 8: Complete installation times](#) on page 64 shows the times for completing each of the above workflows.

Table 8: Complete installation times

Workflow	Time to complete task
Preparation	25 minutes per server
Installation	15 minutes per server
Commissioning	20 minutes

Workflow	Time to complete task
Solution commissioning	4 hours, plus 20 minutes per user

Preparation

This section describes the tasks required to prepare for the installation of the Avaya 3100 Mobile Communicator Gateway.

**Important:**

Use the server system console for installations and upgrades. Do not use a remote terminal.

Before you begin, review [Appendix A: Installation worksheets and checklist](#) on page 163 for useful worksheets and a checklist.

Prerequisites

Obtain a license file for the Avaya 3100 Mobile Communicator Gateway.

Avaya 3100 Mobile Communicator Gateway preparation workflow

[Figure 11: Preparation taskflow](#) on page 66 shows the required procedures.

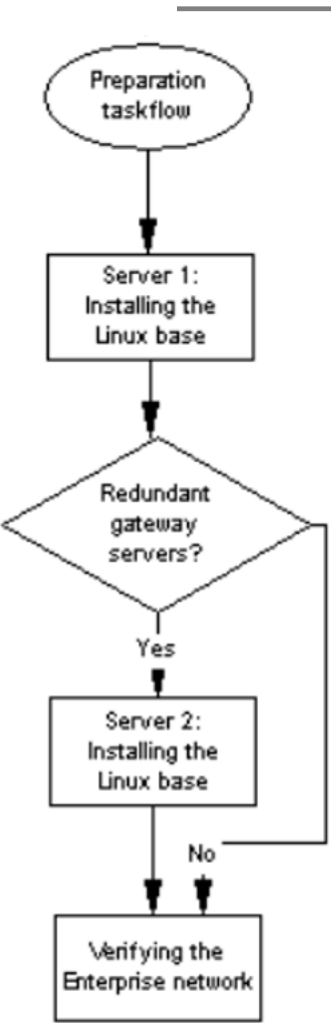


Figure 11: Preparation taskflow

Preparation workflow navigation

- [Installing the Linux base](#) on page 67
- [Verifying the Enterprise network](#) on page 71

[Table 9: Preparation times](#) on page 66 shows the estimated times for completing each of the above procedures.

Table 9: Preparation times

Workflow	Time to complete task
Installing the Linux Base	20 minutes per server
Verifying the enterprise network	5 minutes per server

Installing the Linux base

For installation instructions for the Avaya CS 1000 Linux base, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

Important:

Carefully observe the labels for the network interfaces of the specific platforms.

During the Linux base installation for Avaya 3100 Mobile Communicator Gateway, you make two platform-specific configuration changes.

- Physical connection—Use only the eth1 physical network interface.
 - HP COTS platform—The network interfaces can be labelled (0,1) or (1, 2). The lower number is eth0 and the higher number is eth1.
 - IBM 306M platform—The network interfaces are labelled backwards. Interfaces (0, 1) are eth1 and eth0 respectively.
- IP addresses—During the Linux base installation, the software prompts you to enter the TLAN and ELAN network interface IP addresses.
 - Configure the ELAN network interface IP with an unused private IP address. The IP standard reserves specific address ranges within Class A, Class B, and Class C for use by private networks (intranets). [Table 10: Reserved IP address ranges](#) on page 67 lists the reserved ranges of the IP address space.
 - Configure the TLAN network interface IP to the same IP address as the Avaya 3100 Mobile Communicator Gateway and corresponding physical eth1 network interface.

Table 10: Reserved IP address ranges

Class	Private starting address	Private ending address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Important:

This procedure documents the installation of Avaya Linux base on a commercial off-the-shelf (COTS) server with no previous Avaya Linux base installation.

Connect to the COTS server using a serial console or keyboard, video monitor, and mouse (kvm).

Important:

Before installing the Linux base, read all of the documentation provided by the manufacturer of the COTS server.

1. Insert the Linux base bootable CD-ROM in the CD-ROM tray.
2. Reboot the server.
3. Choose the method of installation:
 - To install using a serial console on COM1, type `com1` at the boot prompt and press `Enter`.
 - To install using an attached keyboard, video monitor, and mouse, type `kvm` at the boot prompt and press `Enter`.

Note: It is not required to attach a keyboard, video monitor and mouse (KVM) to view output. A console-based installation will also provide output.
4. Type `y` and press `Enter`.
5. The Format all partitions screen appears. Press `Enter` to continue.
6. At the prompt, select the type of configuration data you wish to use. Type `1` for Normal installation and press `Enter`, and then press `Enter` again when prompted, as shown in
7. The System Configuration screen appears as shown in . Press `Enter` to continue.

```

#####
#               System Configuration               #
#####

You will now be prompted to enter configuration data for this
server.

Once you have completed the configuration, the installation
will begin.

Throughout the system configuration phase, you will be given
the chance to verify/modify your input in case any mistakes are made
during data entry.

Press the Enter Key to begin configuration...

```

Figure 12: System configuration window

8. When prompted, in the Network configuration screen, enter the customer information for ELAN IP address, ELAN gateway, ELAN netmask, hostname, domain name, Machine TLAN IP address, TLAN gateway, Default gateway, and TLAN netmask .
9. The System Console Redirection screen appears. Select the redirection option and press `Enter` to continue.

Note: This screen appears only if you chose to install using an attached keyboard, video monitor, and mouse.
10. In the Time zone selection screen type the appropriate region number at the prompt and then press `Enter` to continue.

The Time zone selection for region screen appears.

```

Timezone Selection
 1) Africa          2) America          3) Antarctica
 4) Arctic          5) Asia             6) Atlantic
 7) Australia       8) Brazil           9) CET
10) CST6CDT        11) Canada          12) Chile
13) Cuba           14) EET             15) EST
16) EST5EDT        17) Egypt           18) Eire
19) Etc            20) Europe          21) Factory
22) GB             23) GB-Eire         24) GMT
25) GMT+0          26) GMT-0          27) GMT0
28) Greenwich      29) HST             30) Hongkong
31) Iceland        32) Indian          33) Iran
34) Israel         35) Jamaica         36) Japan
37) Kwajalein      38) Libya           39) MET
40) MST            41) MST7MDT         42) Mexico
43) Mideast        44) NZ              45) NZ-CHAT
46) Navajo         47) PRC             48) PST8PDT
49) Pacific        50) Poland          51) Portugal
52) ROC            53) ROK             54) Singapore
55) SystemV        56) Turkey          57) UCT
58) US             59) UTC             60) Universal
61) W-SU           62) WET             63) Zulu
Enter Region (1-63): 20

```

Figure 13: Time zone selection window

11. At the prompt, in the Timezone Selection for Region screen, type the appropriate time zone number and then press `Enter` to continue.
12. In the Configuration Validation 1 screen, type `Y` for yes or `N` for no, and then press `Enter` to confirm the customer information for Machine ELAN IP address, ELAN Gateway, ELAN Netmask, Hostname, FQDN, Machine TLAN IP address, Default TLAN Gateway, TLAN Netmask, and Timezone, as shown in
If you select `N`, edit the information as required and repeat step 10.
13. In the Network Time Protocol (NTP) Configuration screen, type `Y` or `N` to choose the NTP transfer mode for the system. Type 1, 2, or 3 and then press `Enter` to indicate the clock source function of the Linux system.
Note: NTP uses Message Digest Algorithm 5 (MD5) signatures to authenticate the exchange of timestamps when operating in secure mode.
14. In the NTP Clock Source Configuration screen type `E` for an external clock source, or `I` for an internal clock source.
Press `Enter` to continue.
15. At the prompt, type the machine TLAN IP address of the clock source server.
Press `Enter` to continue.
16. At the prompt, configure the primary DNS server IP address.
17. Type `Y` and press `Enter` to configure the Primary DNS server IP address.
OR Type `N` and press `Enter` if you do not want to configure the Primary DNS server IP address.

Note 1: In this example we do not configure the Primary DNS server IP address. If you choose `Y` you receive a prompt to provide the Primary DNS server IP address.

Note 2: You can use Base Manager to modify the static lookup table for host names.

18. In the Configuration Validation 2 screen, type `Y` if the information is correct and press `Enter`, as shown in the

Note: The CLI command `hostconfig` can be used to modify the static lookup table for host names.

The Configuration Validation 2 screen appears with the correct information. Press `Enter` to continue.

19. In the Date and Time Configuration screen, configure the date and time, as shown in

Type `Y` to keep the date and time, and then press `Enter`. To change the date and time, press `N`, make the required changes, and press `Enter`. The Date and Time Configuration screen appears with the new date and time. Press `Enter` to continue.

20. In the Password Configuration screen, at the prompt, enter the root password.

21. Enter the sysadmin password.

22. Enter the nortel password.

23. Press `Enter` to continue. The Configuration File Backup screen appears.

24. From the Configuration File Backup screen, select an option to back up the configuration data.

The naming convention for the Linux base backup archive is `hostname-install-yyyy.mm.dd.hh.MM.ss.tar.gz`. The name for the backup archive is automatically generated and includes the key word `install` to indicate that the archive is generated as part of the installation or upgrade procedure. For example, `hp3-e-install-2008.09.04.18.54.47.tar.gz` is a backup archive name where `hp3-e` is the host name. The archive name begins with the short host name (not the FQDN) and the key word `install`, and contains the following fields:

- `yyyy` - year
- `mm` - month
- `dd` - day
- `hh` - hour
- `MM` - minutes
- `ss` - seconds

Note: Avaya Linux base uses the CLI command `sysbackup` to back up system data to external storage. You can choose to back up the data to a USB device or to an SFTP server.

25. After you back up the configuration data, the Package Installation screen appears. The Post System Configuration screen appears. The system automatically reboots as a Linux server.

Verifying the Enterprise network

Install and configure on the enterprise network:

- Domain Name Server (DNS) (required)
- Lightweight Directory Access Protocol (LDAP) server (optional)



Important:

Avaya recommends that you program the DNS with the IP addresses of the License Server, the primary Enterprise Call Server (ECS), and the alternate ECS.

You should ensure that the DNS and LDAP server can be accessed from the Avaya 3100 Mobile Communicator Gateway.

-
1. Access the Admin shell for your DNS server.
 2. To verify that DNS is functional, use the **ping** command and enter the fully qualified domain name (FQDN) of a server on the network.
 3. To verify communication with the LDAP server, use the **ping** command.

After the installation and commissioning is complete, you can verify that LDAP is working by performing a Corporate Directory (Corp Dir) search from a client.

Job aid: Supported LDAP servers

You can configure the Avaya 3100 Mobile Communicator Gateway server to query a corporate directory so that the mobile clients can use the Directory lookup feature on their devices.

The Directory lookup feature uses LDAP to perform the query on one of the following supported directory servers:

- Active Directory/Exchange Server 2000 or 2003
- Avaya Common Network Directory (CND)—Telephony Manager (TM) 3.1 in Avaya CS 1000 includes CND.

For information about configuring LDAP parameters on the Avaya 3100 Mobile Communicator Gateway, see *Avaya 3100 Mobile Communicator Administration and Security, NN42030-600*.

Installation

This section describes the software installation.



Important:

Use the server system console for installations and upgrades. Do not use a remote terminal.

Installation task flow

[Figure 14: Installation taskflow](#) on page 72 shows the required procedures.

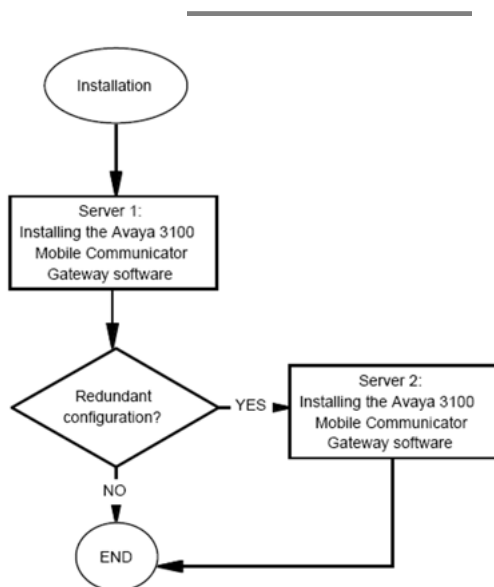


Figure 14: Installation taskflow

Result

Installation workflow navigation

[Installing the Avaya 3100 Mobile Communicator Gateway software](#) on page 73

[Table 8: Complete installation times](#) on page 64 shows the times for completing each of the above procedures.

Job aid: Admin shell access

Many of the maintenance procedures require that you access the admin shell and log on using the nortel user account. You have two options for admin shell access:

- serial port connection
- Secure Shell (SSH)

For more information about accessing the admin shell, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

Installing the Avaya 3100 Mobile Communicator Gateway software

During the software installation, a number of prompts appear. You can either accept the default value or enter a new value at each prompt.

Prerequisites

- You must be logged into the server as nortel. For more information, see [Accessing the server command line as nortel](#) on page 159.
- You must know the root password to perform the following procedure.
- You require a compact disc (CD) containing the Avaya 3100 Mobile Communicator software.

-
1. Insert the Avaya 3100 Mobile Communicator Gateway software CD into the CD-ROM drive of the host server.
 2. Enter the following command:
appinstall
The installation script prompts you for the root password.
 3. Enter the root password.
 4. Read the software license agreement.
 5. To agree to the license agreement, enter **YES**
The software installation proceeds. Messages appear to show installation progress. After the installation completes, the configuration script starts automatically.
 6. At the prompt for the ethernet address, select the card that corresponds to the IP address of this Avaya 3100 Mobile Communicator Gateway server.

7. At the prompt for the mode, do one of the following:
 - If the Avaya 3100 Mobile Communicator Gateway configuration is not redundant, select Standalone mode.
 - If the Avaya 3100 Mobile Communicator Gateway configuration is redundant, select Active-Standby mode, and go to [8](#) on page 74.
 8. For Active-Standby mode, at the prompt, enter the following information:
 - Server name: the domain name (if defined) or the internal IP address of the primary Avaya 3100 Mobile Communicator Gateway. This value is the same for both the primary and secondary Avaya 3100 Mobile Communicator Gateway servers.
 - Cluster name: this value is not currently in use. Use the default value.
 - Partner IP address: the IP address of the other Avaya 3100 Mobile Communicator Gateway server.
 9. Select **Finish** to save the configuration.
 10. Remove the CD.
 11. For a redundant configuration, repeat this procedure on the other server.
-

Commissioning

This section describes the Avaya 3100 Mobile Communicator Gateway commissioning.

After completing the commissioning, you configure the system security, configure the client services, install the clients, and back up the Avaya 3100 Mobile Communicator Gateway database. For more information, see *Avaya 3100 Mobile Communicator Administration and Security, NN42030-600*

After you configure the Avaya 3100 Mobile Communicator solution, you configure the Avaya 3100 Mobile Communicator to interwork with the appropriate communication server, using the appropriate Solution Integration Guide.

Adding an Avaya 3100 Mobile Communicator Gateway server

Add the Avaya 3100 Mobile Communicator Gateway using the Avaya 3100 Mobile Communicator Web Administration Console.

Prerequisites

- The Avaya 3100 Mobile Communicator Gateway software must be installed on the server.
- You must be logged into the Avaya 3100 Mobile Communicator Web Administration Console as administrator. For more information, see [Logging on to the Avaya 3100 Mobile Communicator Web Administration Console as an administrator](#).
- You are familiar with the configuration settings for the Avaya 3100 Mobile Communicator Gateway. For more information, see [Table 11: Avaya 3100 Mobile Communicator Gateway configuration settings](#) on page 76.
- You are familiar with the Device Configuration settings for the Avaya 3100 Mobile Communicator Gateway. For more information, see [Table 12: Device configuration settings](#) on page 84.

-
1. Click the **System Configuration** tab.
 2. On the System Configuration page, select **Gateway Actions > Configure Gateway**.
 3. On the Configure Gateway page, configure the parameters.
 4. Click **Save**.
 5. Click **Close**.
You receive a prompt to restart the server.
 6. At the prompt to restart the gateway, click **Yes**.
The primary and secondary gateway servers restart. Secondary gateway configuration comes from the data you enter for the primary gateway. Secondary gateway configuration is automatic; there is no need to configure it separately.
 7. Click the **Device Configuration** tab.
 8. On the Device Configuration page, configure the parameters for devices.
 9. Click **Save**.
-

Configuring the Gateway settings

Configure the Gateway settings to enable the Avaya 3100 Mobile Communicator Gateway to interact with the network elements. In redundant Avaya 3100 Mobile Communicator deployments, most of the Gateway settings are shared between the two servers.

Prerequisites

You must be logged into the Avaya 3100 Mobile Communicator Web Administration Console as administrator. For more information, see [Logging on to the Avaya 3100 Mobile Communicator Web Administration Console as an administrator](#).

-
1. Click the **System Configuration** tab.
 2. Click **Gateway Actions > Configure Gateway**.
 3. Click **Edit**.
 4. Modify the Gateway settings.

 Important:

Secondary gateway configuration comes from the data you enter for the primary gateway. Secondary gateway configuration is automatic; there is no need to configure it separately.

5. Click **Save**.
6. Click **Close**.
You receive a prompt to restart the server.
7. To restart the system, and apply the updated gateway configuration, click **Yes**.

OR

To restart the system at a later time, click **No**. The updated Gateway settings are applied when the system is restarted later.

In a redundant configuration, both the primary and secondary gateway servers restart.

 Important:

Avaya recommends that you restart the gateway.

Procedure job aid

Use the following table to help you understand the Gateway settings. Use this job aid for Avaya CS 1000 installations only.

Table 11: Avaya 3100 Mobile Communicator Gateway configuration settings

Field	Description
Mobility Server	
SIP Port	Enter the SIP server port. The default value is 5060.

Field	Description
	This parameter applies to both servers in the redundant configuration.
Domain	Enter the SIP registration domain defined on the Enterprise Call Server (ECS). This parameter applies to both servers in the redundant configuration.
Gateway name	Enter the gateway identity defined on the ECS for the Avaya 3100 Mobile Communicator Gateway. This parameter applies to both servers in the redundant configuration.
Media Server Default Locale	Select the media server default locale. The Avaya 3100 Mobile Communicator Gateway plays prompts to the Avaya 3100 MC - Client or Web UI user in the language that the individual user has configured. If that language is not installed on the Avaya 3100 Mobile Communicator Gateway, the prompts play in the language specified in this field. For more information about prompts, see Audio prompt administration .
Media Server	Enter the address and port of the Instant Conferencing Server. Format: <IP address FQDN> :<port> This parameter is unique to the local server.
Incoming Call Reliable Timer	Specify the amount of time, in seconds, that the Avaya 3100 Mobile Communicator Gateway waits after it plays the cellular voice mail avoidance prompt, while waiting for the pound (#) key to be pressed, before the call forwards to the Enterprise voice mail system. This parameter applies to both servers in the redundant configuration.
Enable Cellular Voicemail Avoidance	Select Yes to route unanswered cell phone calls to the enterprise voice mail system. Select No to route unanswered cell phone calls to the cellular voice mail system. When call screening mode is disabled, this parameter controls whether an unanswered, incoming call diverts to the enterprise voice mail system or to the cellular voice mail system. Default: No
Enable Music on Hold	Select Yes to enable the Music on Hold feature. The system must have an audio file installed containing the music to be played to the caller when on hold. Select No to disable the Music on Hold feature. Default: Yes
Primary ECS Address	Enter the address and port of the primary ECS. Format: <IP address FQDN> :<port>

Field	Description
	This parameter applies to both servers in the redundant configuration.
Secondary ECS Address	Enter the address and port of the secondary ECS. Format: <IP address FQDN> :<port> This parameter applies to both servers in the redundant configuration.
Device Access	
HTTP Port	Select the hypertext transport protocol (HTTP) port used by clients to access the system and to download software over the air. The valid range is 8080 to 8089; the default is 8080. Select 0 to disable the port. This parameter applies to both servers in the redundant configuration.
HTTPS Port	Select the HTTP Secure (HTTPS) port used by clients to access the system and to download software over the air. The valid range is 8440 to 8449; the default is 8443. Select 0 to disable the port. Use HTTPS when a certificate infrastructure exists on the clients and Avaya 3100 Mobile Communicator Gateway. This parameter applies to both servers in the redundant configuration.
HTTPS certificate password	Enter the password used for the HTTPS certificate transmitted by clients to the Avaya 3100 Mobile Communicator Gateway server. The default is <i>nortel</i> . This parameter applies to both servers in the redundant configuration.
Dial Plan	
User Prefix/Phone-context for Call Origination	Enter the user name prefix or phone context for call origination. This prefix applies to calls originated by the Avaya 3100 Mobile Communicator Gateway server and to the calling address. This parameter applies to both servers in the redundant configuration.
Mobility Prefix	Enter the user name mobility prefix for call termination. This prefix applies to calls received by the Avaya 3100 Mobile Communicator Gateway server and to the called address. This parameter applies to both servers in the redundant configuration.
Dial-In Service DN	Enter the Service Directory Number (DN) for client calls that will arrive at the Avaya 3100 Mobile Communicator Gateway on the SIP network. This field is mandatory. The Service DN allows Avaya 3100 MC - Client for

Field	Description
	BlackBerry, Avaya 3100 MC - Client for Windows Mobile, and Avaya 3100 MC - Client for Nokia users to place calls directly from their wireless devices to other parties using the client's Direct Outbound call mode. The PSTN numbers that are dialed by the mobile on the PSTN are defined on the device configuration page. When the call arrives at the enterprise the PSTN number must be converted to an internal format for use on the SIP network, routed by the NRS, and which will eventually arrive at the Avaya 3100 Mobile Communicator Gateway. Mobility Prefix: 888 Username 343XXXX Password XXXXXXX Outgoing Call Service DN +15066404681 The mobile phone will dial +15066404681 for direct outbound calls. This PSTN number will be routed to the enterprise as a DID number. When the number arrives at the Enterprise we must manipulate the PSTN number (+15066404681 to be routed on the SIP network.  Important: If you have a mapping on the incoming trunk route on the call server to map a PSTN service DN number: +15066404681 to 8885066404681, you would configure the service DN on the Avaya 3100 Mobile Communicator Gateway as 5066404681. In the case where an enterprise has multiple service DN's all incoming PSTN service DN calls must map to the single service DN number configured in this field. For example: +1613132 4567 to 8885066404681.
Dialplan Conversion List	For information about configuring this field, see Configuring the dial plan conversion parameters on page 81.
DTR	
Initial port for DTR (27000-27499)	Enter the first port in the range of ports used by the Avaya 3100 Mobile Communicator Gateway server Digital Tone Receiver (DTR) engine. A DTR recognizes Dual Tone Multi-Frequency (DTMF). 1500 ports are allotted for DTR. The port must be an even number (for example, 27000). This parameter applies to both servers in the redundant configuration.
Mid-Call Cellular Prefix	Enter the prefix used by clients to invoke mid-call features using DTMF. Permitted values include the characters star (*) and pound (#), and the numerals 0 to

Field	Description
	9, entered in any combination. The default value is *, which needs to be changed only if it conflicts with other network resources. For example, if clients use * to access conference features, then you must change the Mid-Call Cellular Prefix to a different value such as # or #99. This parameter applies to both servers in the redundant configuration.
LDAP	
URL	Enter the address and port of the Lightweight Directory Access Protocol (LDAP) server that hosts the corporate directory. Obtain this value from the directory administrator. Format: ldap://<IP address FQDN>:<port> This parameter applies to both servers in the redundant configuration.
Search Base	Enter the distinguished name of the search base object (node) that defines the location in the directory from which the LDAP search begins. Obtain this value from the directory administrator. This parameter applies to both servers in the redundant configuration.
LDAP Username	Enter the user name required to gain access to the LDAP server that hosts the corporate directory. Obtain this value from the directory administrator. This parameter applies to both servers in the redundant configuration.
Authorization	Enter the authorization mechanism required to connect to the LDAP server. The default value is <i>simple</i>, which causes user names and passwords to be sent as clear text. This parameter applies to both servers in the redundant configuration.
Password	Enter the password required to gain access to the LDAP server that hosts the corporate directory. Obtain this value from the directory administrator. This parameter applies to both servers in the redundant configuration.
LDAP attribute tag that contains the user ID	Enter the tag for the User ID attribute on the LDAP server. The default is <i>ipPhone</i>. This parameter applies to both servers in the redundant configuration.
LDAP attribute tag that contains the user's first name	Enter the tag for the User First Name attribute on the LDAP server. The default is <i>givenName</i>. This parameter applies to both servers in the redundant configuration.

Field	Description
LDAP attribute tag that contains the user's last name	Enter the tag for the User Last Name attribute on the LDAP server. The default is sn. This parameter applies to both servers in the redundant configuration.
LDAP attribute tag that contains the user's display name	Enter the tag for the User Display Name attribute on the LDAP server. The default is displayName. This parameter applies to both servers in the redundant configuration.
LDAP attribute tag that contains the user's business phone #	Enter the tag for the User Business Phone Number attribute on the LDAP server. The default is telephoneNumber. This parameter applies to both servers in the redundant configuration.
LDAP attribute tag that contains the user's mobile phone #	Enter the tag for the User Mobile Phone Number attribute on the LDAP server. The default is ipPhone. This parameter applies to both servers in the redundant configuration.
LDAP attribute tag that contains the user's email address	Enter the tag for the User E-mail Address attribute on the LDAP server. The default is email. This parameter applies to both servers in the redundant configuration.
LDAP attribute tag that contains the user's extension	Enter the tag for the User Extension attribute on the LDAP server. The default is ipPhone. This parameter applies to both servers in the redundant configuration.
LDAP attribute tag that contains the user's home phone	Enter the tag for the User Home Phone Number attribute on the LDAP server. The default is homePhone. This parameter applies to both servers in the redundant configuration.

Configuring the dial plan conversion parameters

Use this procedure to facilitate dial plan conversion.

Prerequisites

- You must be logged into the Avaya 3100 Mobile Communicator Web Administration Console as administrator. For more information, see [Logging on to the Avaya 3100 Mobile Communicator Web Administration Console as an administrator](#).
- Understand the dial plan of the Enterprise Call Server (ECS). For more information, see *Avaya Communication Server 1000 Dialing Plans Reference, NN43001-283*.
- Understand the format of telephone numbers in the corporate directory server.

1. Click the **System Configuration** tab.
2. Select **Gateway Actions > Configure Gateway**.
3. Click **Edit**.
4. Click the corresponding link for **Dialplan Conversion List**.

Dial Plan

User Prefix/Phone-context for Call

Mobility Prefix

Dial-In Service DN

Dialplan Conversion List

506=61506 Add

Cancel OK

cdp.udp

888

5066404681

[no values have been set...](#)

Figure 15: Dialplan conversion list

5. In the **Number** box, type a number combination, and then click **OK**.
6. For each additional entry, click **New Entry** and in the **Number** box, type a new number combination.
7. To save the changes, click **OK**.
8. Click **Save**.

Variable definitions

Variable	Description
<i><number combination></i>	Represents the elements of a dialable number and what these elements translate to in order to be dialed. Format: <original combination>=<converted number> Example: ESN=6 If the corporate directory gives a telephone number as ESN1234567, the ESN is changed to the digit 6 when the number is dialed, resulting in the number 61234567 being dialed.

Rules that use the carat sign

When you write a rule without the carat (^) sign, the Avaya 3100 Mobile Communicator Gateway replaces all occurrences of what is on the left side of the equal (=) sign with what is on the right. For example, if you have the following rule 0=00, the rule changes a phone number dialed on the Avaya 3100 MC - Client as 0123456789 to 00123456789 but also changes a phone number like 01230123 to 0012300123

When you write a rule with the ^ sign, the Avaya 3100 Mobile Communicator Gateway replaces only the leading occurrence of the string of what is on the left side of the equal (=) sign with what is on the right. For example, you have a rule ^0=00. If the phone number dialed on the Avaya 3100 MC - Client is 0123456789, the number changes to 00123456789. However, if the phone number dialed is 01230123, the number changes to 001230123.

You can use the ^ sign when writing rules in North America or Europe to dial national numbers without adding the access code of 1 used within the enterprise. You can write a rule to look for a leading 0 in Europe or 1 in North America and insert the proper access code to make the number dialable in the enterprise. For example, in North America the rule would be ^1=61 assuming an access code of 6. This takes a number dialed as 16131234567 and substitutes 6161231234567 to make the number dialable in the enterprise. In Europe, this same rule would be ^0=00. This adds an extra 0 to any number that a user dials on the Avaya 3100 MC - Client. For example, 0123456789 becomes 00123456789 or 00411234567890 becomes 00041123456789.

Configuring the device settings

The mobile device settings can automatically download to all the clients. A null value downloads if a parameter is not configured.

The device configuration page is the list of configuration settings that are downloaded to the device each time at login. You can change this behavior so that settings only download when the user first logs in.

Prerequisites

- You must be logged into the Avaya 3100 Mobile Communicator Web Administration Console as administrator. For more information, see [Logging on to the Avaya 3100 Mobile Communicator Web Administration Console as an administrator](#).
- Add and configure the Avaya 3100 Mobile Communicator Gateways before you begin this procedure. For more information, see [Adding an Avaya 3100 Mobile Communicator Gateway server](#) on page 74.

-
1. Click the **Device Configuration** tab.

Figure 16: Device configuration tab

2. Click **Edit**.
3. Modify the Device settings.
4. Click **Save**.

The new device settings apply for the next successful logon by each user. On a redundant system, the gateways automatically share the device settings.

Procedure job aid

Use the following table to help you understand the Devices settings.

Table 12: Device configuration settings

Field	Description
Primary 3100 MCG (all configurations)	
External: Address (IP/host:Port)	Enter the address of the primary Avaya 3100 Mobile Communicator Gateway public interface on the Internet. Client application users connect to this address. Format: <IP address FQDN> :<port>

Field	Description
External: Use Secure Connection	Select Yes to enable HTTPS connections on the primary Avaya 3100 Mobile Communicator Gateway public interface using security certificates on the clients on Avaya 3100 Mobile Communicator Gateway. Select No to enable HTTP. Use HTTPS when the clients use certificates to encrypt communication with the Avaya 3100 Mobile Communicator Gateway. The Nokia and Windows Mobile devices, along with BlackBerry devices that do not employ the enterprise-hosted BlackBerry Enterprise Server (BES), can use HTTPS and certificates. Default: Yes
Internal: Address (IP/host:Port)	Enter the address of the primary Avaya 3100 Mobile Communicator Gateway private interface on the network. Configure this parameter if your Avaya 3100 Mobile Communicator system implementation uses BlackBerry devices that use the BES.
Internal: Use Secure Connection	Select Yes to enable HTTPS connections on the primary Avaya 3100 Mobile Communicator Gateway private interface. Select No to enable HTTP. Default: No
Secondary 3100 MCG (all configurations)	
External: Address (IP/host:Port)	Enter the address of the secondary Avaya 3100 Mobile Communicator Gateway public interface on the Internet. Client application users connect to this address when the primary Avaya 3100 Mobile Communicator Gateway fails. Format: <IP address FQDN> :<port>
External: Use Secure Connection	Select Yes to enable HTTPS connections on the secondary Avaya 3100 Mobile Communicator Gateway public interface using security certificates on the clients on Avaya 3100 Mobile Communicator Gateway. Select No to enable HTTP. Use HTTPS when the clients use certificates to encrypt communication with the secondary Avaya 3100 Mobile Communicator Gateway. The Nokia and Windows Mobile devices, along with BlackBerry devices that do not employ the enterprise-hosted BlackBerry Enterprise Server (BES), can use HTTPS and certificates. Default: Yes
Internal: Address (IP/host:Port)	Enter the address of the secondary Avaya 3100 Mobile Communicator Gateway private interface on the network.

Field	Description
	Configure this parameter if your Avaya 3100 Mobile Communicator system implementation uses BlackBerry devices that use the BES.
Internal: Use Secure Connection	Select Yes to enable HTTPS connections on the secondary Avaya 3100 Mobile Communicator Gateway private interface. Select No to enable HTTP. Default: No
Access Numbers	
Voicemail Numbers	Enter the list of valid regional or office based numbers users of the system can use to call and access their voice mail.
Service Numbers	Enter the list of valid regional or office-based Direct Outbound Mode numbers for client calls. These numbers are PSTN/E.164 numbers. Avaya 3100 Mobile Communicator users use service numbers to place calls directly from their wireless devices to other parties using Direct Outbound call mode. On the Avaya CS 1000, the PSTN number must map to the gateway name assigned to the Avaya 3100 Mobile Communicator Gateway as a trunk steering code. On the Avaya CS 1000, the PSTN number must map to the number populated in table DNROUTE of the Avaya CS 1000.
Mobile Network Dialing	
Emergency and Direct Dialed Numbers	Click to add new entries to the list of emergency or direct dialed numbers. You can remove entries from the list by clicking the corresponding x.
Auto-Download of Device Configuration	
Allow Client Override	Controls the automatic downloading of the device configuration (including blank values) to the clients. Select No to download the configuration every time a user logs in. The download overwrites local updates. Select Yes to download the configuration the first time each user logs in. After the initial download, users can change their configuration. Default: No
Calling Features	
Prefix Screen Setting	Controls the use of prefixes by users. Select Disable to allow users to dial outgoing calls with prefixes. For this setting and the Native Call Intercept setting to work correctly, your dial plan must support calls from the client in the same way that calls from the native dialer are handled.

Field	Description
	Select Enable to require users to enter a prefix every time they make an outgoing call. This setting is useful if your dial plan does not support E.164 numbers. Default: Disable
Default for Native Call Intercept Setting	Defines the default setting to control the ability for users to make private calls that route through the Avaya 3100 Mobile Communicator Gateway. Private calls are calls placed through the native dialer. Select On to place private calls through the Avaya 3100 Mobile Communicator Gateway. Select Off to place private calls through the native dialer. The user can override this setting on the client. If the user overrides this setting, changes to this parameter do not change the client configuration. Default: On

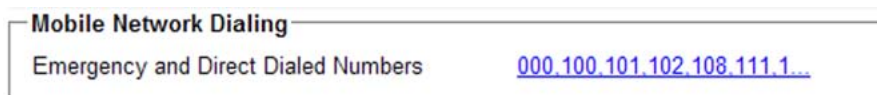
Configuring the emergency telephone numbers

Add one or more entries to facilitate emergency number dialing from the device's native phone.

Prerequisites

- You must be logged into the Avaya 3100 Mobile Communicator Web Administration Console as administrator. For more information, see [Logging on to the Avaya 3100 Mobile Communicator Web Administration Console as an administrator](#).
- You must know the emergency telephone numbers for your location.

1. Select the Device Configuration tab.
2. Click **Edit**.
3. Click the corresponding link for **Emergency and Direct Dialed Numbers**.



4. In the **Number** box, type an emergency number, and then click **OK**.
For example, to enable emergency number dialing in North America, add 911. When a mobile client user dials that number, the Avaya 3100 MC - Client switches to the native device phone and places the call over the cellular network.
5. For each additional entry, click **New Entry** and in the **Number** box, type a new number combination.

6. To save the changes, click **OK**.
7. Click **Save**.

Adding the Avaya 3100 Mobile Communicator Gateway license

This procedure installs the license file on the Avaya 3100 Mobile Communicator Gateway. This license file controls the number of users that can log in to the system.

Prerequisites

- You must be logged into the Avaya 3100 Mobile Communicator Web Administration Console as administrator. For more information, see [Logging on to the Avaya 3100 Mobile Communicator Web Administration Console as an administrator](#).
- Obtain a license file from Avaya before beginning this procedure.
- Add the Avaya 3100 Mobile Communicator Gateway server before beginning this procedure.

1. Add the license file to a directory on your network that is accessible from the Avaya 3100 Mobile Communicator Gateway.
2. Click the **System Configuration** tab.
3. In the **System Configuration** page, click **Gateway Actions, License** beside the Avaya 3100 Mobile Communicator Gateway.

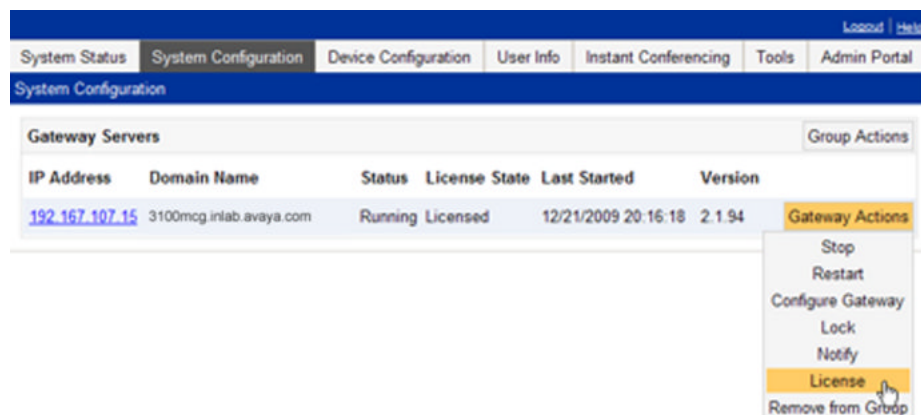


Figure 17: Gateway Actions

4. In the **License Information** window, click **Browse**.
5. In the **Choose file** dialog box, locate and select the license file.

6. Click **Open**.
7. Click **Install**.
8. Click **Close**.
9. On a redundant system, repeat step [3](#) on page 88 to step [8](#) on page 89 on the second server.

! Important:

For information about troubleshooting license file problems, see *Avaya 3100 Mobile Communicator Troubleshooting, NN42030-700*.

Checking Gateway server status

Check the Gateway server status to view the information such as the number of connections and the system load.

The System Status page lists the server processes and autoupdates every five seconds.

Prerequisites

You must be logged into the Avaya 3100 Mobile Communicator Web Administration Console as administrator. For more information, see [Logging on to the Avaya 3100 Mobile Communicator Web Administration Console as an administrator](#).

1. Click the **System Status** tab.
- The System Status window appears.

IP Address	Domain Name	Status	Last Alarm Entry	Active Connections	Queued Messages	System Load	Tx (kbps)	Rx (kbps)
192.167.107.15	3100mcg.inlab.avaya.com	Running	12/21/2009 20:16:59 (2)	0	0	0.00	0.00	0.00

License Used/Limit: Single: 0/30

Figure 18: System status tab

2. On the System Status page, monitor the status of the Gateway Server.

Procedure job aid

Use the following table to help you understand the Gateway Server System status fields.

Field	Description
IP Address	Contains the IP Address of the Gateway Server. Status information appears to the right of this field. Click the IP Address to view statistical data related to the associated server. If the IP Address displays in red, the server is not responding, which can indicate a server software problem or system outage. If the IP Address displays in grey, the server is unavailable.
Domain Name	Contains the Domain name for the Avaya 3100 Mobile Communicator Gateway server.
Status	Indicates the status of the Gateway Servers. • Running—The server is running and active. • Network Error—Connectivity to the server has been lost. • Stopped—The server is stopped. • Running-Standby—The server is in standby mode. If users cannot log in for any reason, the gateway status appears in red. If the server is running but needs a restart (for example, to apply pending configuration changes), the gateway status appears in orange and an asterisk (*) appears beside the text.
Last Alarm Entry	Click this field to open the alarm log file. The timestamp (MM/DD/YYYY HH:MM:SS) indicates the time of the most recent SEVERE or WARNING alarm message. The total number of outstanding alarms appears in brackets. For example, (5) indicates that five alarms have been raised but not yet cleared. Message examples: • The “MandatoryGatewayConfig” alarm indicates that you must enter configuration settings and restart the server. • The “GatewayStopped” information message indicates that the server has been stopped from the Web Administration Console or command line. Notes:

Field	Description
	• You can access the alarm log file from the Tools page under Server Logs. • To clear an alarm, you must solve the original error condition. • Whenever the Avaya 3100 Mobile Communicator Gateway server stops, all alarms and informational messages clear. However, persistent error conditions (such as missing or incorrect configuration settings) immediately generate new alarms. To permanently delete an alarm, you must solve the original error condition. • Recurrent events only generate one alarm.
Active Connections	Indicates the current number of active connections (clients) handled by the server. The license key determines the maximum number of connections.
Queued Messages	Indicates the current number of queued message waiting to be sent from the server to the client. The CPU and number of server processes determines the maximum number of queued messages. A large number of queued messages can be caused by network congestion or by users having lost service. If the queue reaches the maximum number, system stability can be compromised. You can check the message queue for individuals or clear the message queue for individual users.
System Load	Indicates the current load on the server CPU, expressed as a percentage, averaged over the last minute. The system load indicates the average number of processes that are currently running on the system. A system load exceeding 100% adversely affects system performance.
Tx(kbps)	Indicates the current number of messages transmitted by the server, expressed in kilobits per second (kbps), averaged over the preceding minute.
Rx(kbps)	Indicates the current number of messages received by the server, expressed in kbps, averaged over the preceding minute.
Licenses Used/Limit	Displays the current number of licenses used against the total number of licenses available.

Solution commissioning

This section describes the final steps required to obtain a fully-working Avaya 3100 Mobile Communicator (Avaya 3100 Mobile Communicator) system. You perform these steps in order to have the system working with your Enterprise infrastructure.

Before you perform these steps, the Avaya 3100 Mobile Communicator Gateway must be installed, commissioned, and configured. For more information, see [Avaya 3100 Mobile Communicator Gateway installation workflow](#) on page 63 and *Avaya 3100 Mobile Communicator Administration and Security, NN42030-600*.

In order to get a fully-working Avaya 3100 Mobile Communicator system, you must do the following commissioning steps:

1. On the firewall, configure the Avaya 3100 Mobile Communicator Gateway server private addresses (on the Enterprise network) to the firewall public address (on the internet).

For more information, see the firewall documentation.

2. On the Intranet Domain Name Server (DNS):
 - Program a DNS entry to map to the internal IP address of the Avaya 3100 Mobile Communicator Gateway.
 - Ensure that the Avaya 3100 Mobile Communicator Gateway can access the DNS using port 53 through any firewalls that are in the network.

For more information, see the DNS documentation.

3. On the Enterprise Call Server (ECS):
 - Assign a call service directory number for the Avaya 3100 Mobile Communicator Gateway.
 - Create a route that enables the Avaya 3100 Mobile Communicator Gateway to reach the ECS.
 - Create a user ID that enables the Avaya 3100 Mobile Communicator Gateway to register with the ECS.

For more information, see [Deployment planning](#) on page 47.

4. If using the BlackBerry Enterprise Server (BES), the RIM MDS service must be enabled.
5. If required, implement a certificate infrastructure.

For more information, see *Avaya 3100 Mobile Communicator Administration and Security*, NN42030-600.

6. After the interworking with the network is functioning correctly, send e-mail messages to users that explain how to install and configure their clients.

For more information, see *Avaya 3100 Mobile Communicator Administration and Security*, NN42030-600.

For more information about interworking with the Avaya CS 1000, see *Avaya 3100 Mobile Communicator and Avaya Communication Server 1000 Solution Integration Guide*, NN49000-315.

For more information about interworking with the Avaya CS 1000, see [Interworking requirements with CS 1000](#) on page 29.



Important:

After you have a working Avaya 3100 Mobile Communicator system, back up the Avaya 3100 Mobile Communicator Gateway. For the backup procedure, see [Backing up the Avaya 3100 Mobile Communicator Gateway server databases](#) on page 160.

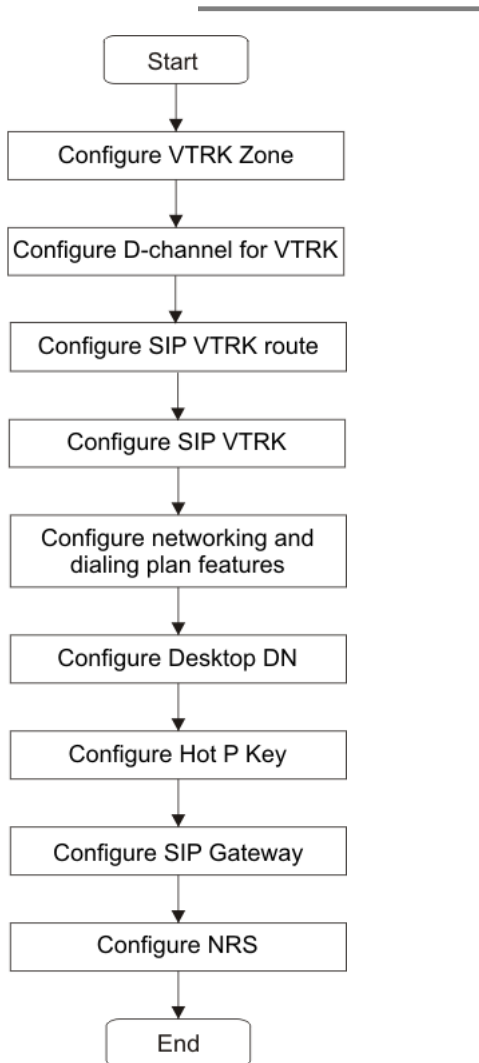
Chapter 11: Avaya CS 1000 configuration for client support

Before implementing IP Peer Networking with the Avaya 3100 Mobile Communicator Gateway, some prerequisite programming is required on the Call Server.

This section assumes that the system is already installed and fully operational, that the Customer data Block (CDB) already exists, and the circuit-switched routes and trunks are already defined. Although you can configure the system using the software overlays (LDs), the procedures here are described using Element Manager.

Avaya CS 1000 configuration for client support task flow

Follow the procedures in the task flow to configure the Avaya CS 1000.



Task flow navigation

Complete the tasks in the order that they appear in the following list:

- [Configuring zones](#) on page 97
- [Configuring a D-channel for virtual trunks](#) on page 97
- [Configuring virtual routes](#) on page 98
- [Configuring virtual trunks](#) on page 100
- [Configuring network control parameters data block](#) on page 101
- [Configuring ESN access codes](#) on page 101
- [Configuring the Route List Block](#) on page 102
- [Coordinated Dialing Plan](#) on page 103

- [Forwarding Service DN to Avaya 3100 Mobile Communicator Gateway](#) on page 103
 - [Configuring a Handoff key](#) on page 105
 - [Configuring a HOT P key](#) on page 106
 - [Configuring the SIP trunk gateway](#) on page 107
 - [Configuring NRS](#) on page 112
-

Configuring zones

For information about configuring zones, see *Converging the Data Network for VoIP Fundamentals, NN43001-260*.

Virtual Trunks must be configured with a different zone number than the endpoints.

Zone Number (ZONE):

Intrazone Bandwidth (INTRA_BW):

Intrazone Strategy (INTRA_STGY):

Best Quality (BQ)Best Bandwidth (BB) Interzone Bandwidth (INTER_BW):

Interzone Strategy (INTER_STGY): Best Quality (BQ)Best Bandwidth (BB)

Resource Type (RES_TYPE): Shared (SHARED)Private (PRIVATE)

Zone Intent (ZBRN): MO (MO)BMG (BMG)VTRK (VTRK)

Description (ZDES):

Configuring a D-channel for virtual trunks

The NRS-SPS application requires Virtual Trunks (routes) to communicate with the Call Server. Virtual Trunks require D-Channels for control and signaling information. Configure the Virtual D-channels in Element Manager or LD 17 (ADAN gate opener).

The calls that use the virtual trunk on the Avaya CS 1000 are:

- calls from the UEXT to Avaya 3100 Mobile Communicator Gateway (mobility prefixed)
- calls from the DID service DN to Avaya 3100 Mobile Communicator Gateway (mobility prefixed)
- calls from the Avaya 3100 Mobile Communicator Gateway outbound

Use this procedure to configure a Virtual D-channel using Element Manager.

-
1. Log on to Element Manager.
 2. In the navigation pane, select **Routes and Trunks, D-Channels**.
If this is the first time that this Web page is accessed, a message indicates that no D-channels are configured. Click **OK**.
 3. Under the Configuration section, from the **Choose a D-channel Number** list, select a D-Channel number.
 4. From the **type** list, select the type of D-Channel.
 5. Click **to-Add**.
 6. Choose the **D channel Card Type (CYTP)** of **D-Channel is over IP (DCIP)**.
 7. Choose the **Interface type for D-channel (IFC)** of **Meridian Meridian1 (SL1)**.
 8. If you are defining the Network Name Display, from the **Release ID of the switch at the far end (RLS)** list, select the release ID of the switch.
 9. Click the **Basic options (BSCOPT)** link. The Basic options (BSCOPT) list expands.
 10. Click **Edit** to configure Remote Capabilities (RCAP).
The Remote Capabilities Configuration page appears.
 11. Select the **Message waiting interworking with DMS-100 (MWI)** check box.
 12. Select the **Network name display method 2 (ND2)** check box.
 13. At the bottom of the Remote Capabilities Configuration page, click **Return - Remote Capabilities**.
The D-Channel xx Property Configuration page reappears.
 14. Click **Submit** to save the changes.
The D-Channels page reappears with the changes.
-

Configuring virtual routes

To configure Virtual Trunk routes, you can use Element Manager or LD 16 of the Command Line Interface.

Note: The zone parameter makes the codec selections and calculates the bandwidth usage for calls to the trunk members of a given route.

Use this procedure to configure a Virtual Trunk Route using Element Manager.

-
1. Select **Routes and Trunks , Routes and Trunks** from the EM Navigator.

The Routes and Trunks Web page opens.

2. Click **Add route associated with the customer**.

The Customer xx, New Route Configuration Web page opens (where xx is the customer number).

3. Under Basic Configuration, fill in the required fields to create a new Virtual Trunk Route:

- Select a Route Number (ROUT) from the drop-down list.
- Select the Trunk Type (TKTP) = TIE trunk data block (TIE). When Trunk Type (TKTP) is selected, the following three options appear:
 - The route is for a virtual trunk route (VTRK) (see step 4)
 - Digital Trunk Route (DTRK)
 - Integrated Services Digital Network option (ISDN) (see step 5)
- Enter the Access Code for the trunk route (ACOD).

4. Select **The route is for a virtual trunk route (VTRK)** check box. The following three fields display:

- Enter a ZONE number.
- Enter the NODE ID (the node served by this Signaling Server).
- Select the Protocol ID for the route (PCID). Select SIP from the two available options.

Note: When SIP is selected as the Protocol ID for the route (PCID), then the Print Correlation ID in CDR for the route (CRID) check box is displayed. CRID only appears if VTRK is YES and PCID is SIP and CDR is turned on for the route.

5. Select the **Integrated Services Digital Networks option (ISDN)** check box.

The ISDN section expands with:

- Choose Mode of operations (MODE) = Route uses ISDN Signaling Link (ISLD).
- Choose Interface type for route (IFC) = Meridian M1 (SL1)
- Select the Network Calling Name Allowed (NCNA) check box

6. Select the **Network Call Redirection (NCRD)** check box.

7. Click Network Options.

8. Select Signaling arrangement (SIGO) = DTI data calls plus all other types (ESN5).

9. Click **General Options**.

The General Options list expands.

10. Enter the Trunk Access Restriction Group (TARG) value if you are configuring a single customer.

11. Enter the appropriate information in the text boxes and in Basic Route Options, Network Options, General Options, and Advanced Configurations.
 12. Click **Submit**.
The Trunks and Routes Web page opens and the newly configured route is displayed for the customer.
-

Configuring virtual trunks

To configure Virtual Trunk, you can use Element Manager or LD 14 of the Command Line Interface.

Use this procedure to configure a Virtual Trunk using Element Manager.

-
1. Select **Routes and Trunks, Routes and Trunks** from the EM Navigator.
The Routes and Trunks Web page opens.
 2. Select the Customer.
 3. Click **Add trunk** associated with the VTRK route the trunks are being added to.
The New Trunk Configuration Web page opens.
 4. Under Basic Configuration, fill in the required fields to create the new Virtual Trunk.
 - Choose Multiple trunk input number (MTINPUT) = 32
 - Choose Trunk data block (TYPE) = IP Trunk (IPTI)
 - Enter the Terminal Number (TN)
 - Enter the Route number, Member number (RTMB)
 - Choose a Card Density (CDEN) of Octal Density (8D)
 - Choose a Start arrangement Incoming (STRI) = Wink OR Fast Flash (WNK)
 - Choose a Start arrangement Outgoing (STRO) = Wink OR Fast Flash (WNK)
 - Enter the Trunk Group Access Restriction (TGAR)
 - Enter the Channel ID for this trunk (CHID)

Note: When creating multiple virtual trunks, select a CHID of 1. The software auto fills the CHID for the additional trunks.

Configuring network control parameters data block

To configure Network Control Parameters data block, you can use Element Manager or LD 87 of the command line interface (CLI).

You must create a Network Control Parameters (NCTL) data block, if one does not exist.

Use this procedure to create a Network Control Parameters (NCTL) data block using Element Manager.

-
1. Log on to Element Manager.
 2. In the navigation pane Dialing and Numbering Plans, select **Electronic Switched Network, Network Control & Services, Network Control Parameters (NCTL)**.
If the Network Control Parameters data block does not exist you are prompted to add one.
The Network Control Parameters page opens.
 3. Click **Submit** to accept the defaults and create the NCTL data block.
-

Configuring ESN access codes

Use this procedure to configure the ESN access codes and basic parameters using Element Manager.

-
1. Log on to Element Manager.
 2. In the navigation pane Dialing and Numbering Plans, select **Electronic Switched Network, Network Control & Services , ESN Access Code and Basic Parameters**.
Note: If the ESN data block does not exist you are prompted to add one. The ESN Access Code and Basic Parameters page opens.
 3. Configure ESN Access Code and Basic Parameters.
 - Choose Maximum number of Digit Manipulation tables (MXDM).
 - Choose Maximum number of Route Lists (MXRL).

Note: If MXRL = 0, the system does not allow the creation of any route lists.

- Enter a NARS/BARS Access Code (AC1) of up to four digits. Typically, the number is 9 for North America.

Note: The code cannot conflict with any value in the numbering plan.

- Enable Coordinated Dialing Plan feature for this customer (CDP). When enabled two additional fields appear.

- Choose Maximum number of Steering Codes (MXSC)

Note:

Steering Codes are part of the customer numbering plan. Ensure the digits used are available in the Numbering Plan at each site in the CDP network.

- Choose Number of digits in CDP DN (DSC + DN or LSC + DN) (NCDP)
Identify the number of CDP digits dialed in an on-net CDP call. Typically, the number is 4.

Configuring the Route List Block

Use this procedure to configure the Route List Block (RLB) to ensure proper call routing.

-
1. Log on to Element Manager.
 2. In the navigation pane Dialing and Numbering Plans, select **Electronic Switched Network, Network Control & Services, Route List Block**.
Note: If Route List Blocks are not configured, the `Route List does not exist` error message appears. Click **OK**.

3. Enter a Route List Index number.

4. Click **to Add**.

The Route List Block Configuration page appears.

Note: If this is the first time that this Web page is accessed, a message indicates the Customer has no data blocks of the correct type. Click **OK**.

5. Enter a Route List Index (RLI) number.
6. Select the Route Number (ROUT) previously defined for virtual trunking.
7. For Strategy on Congestion (SBOC), select Reroute All (RRA).

8. Accept all other defaults.
 9. Click **Submit**.
-

Coordinated Dialing Plan

A Coordinated Dialing Plan (CDP) permits a customer to define a simple dialing plan for an entire network. Each user within the network is assigned a unique 3-10 digit telephone number that does not conflict with any other in the network. All telephone numbers at a particular location must be the same length.

A calling party at one node calls a destination party at another node by simply dialing the telephone number assigned to the destination party. No access codes or pauses for dial tone are required with CDP.

A Coordinated Dialing Plan telephone number is composed of a unique 1-7 digit prefix, known as a Steering Code, which identifies the network node on which an extension is located, followed by the remaining digits that uniquely identify the extension. A Steering Code cannot be the same as any access code or other extension number.

There are three types of Steering Codes:

- Distant Steering Code
- Local Steering Code
- Trunk Steering Code

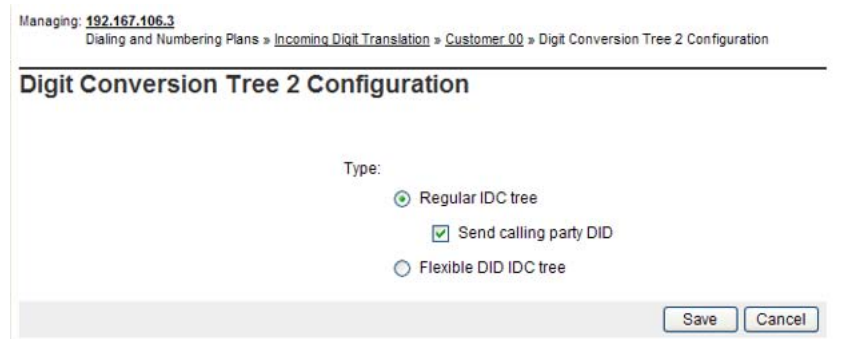
When using a CDP, you must use CDP steering codes. Distant Steering Codes (DSC) are the most common.

Forwarding Service DN to Avaya 3100 Mobile Communicator Gateway

Use this procedure to forward the Service DN to the Avaya 3100 Mobile Communicator Gateway.

-
1. Log on to Element Manager.
 2. In the navigation pane **Customers, Customer 00** ., **Edit** , **Feature Packages**
 3. Enable packages:
 - New Flexible Code Restriction (NFCR) package 49
 - Incoming Digit Conversion (IDC) package 113

4. In the navigation pane **Dialing and Numbering Plans**, **Incoming Digit Translation**
5. Click **Customer Edit IDC**.
The Incoming Digit Conversion Property page opens.
6. Choose **Digit Conversion Tree Number**. Click **New DCNO**.
7. Enable Type: **Send calling party DID**.



Managing: [192.167.106.3](#)
Dialing and Numbering Plans » Incoming Digit Translation » Customer 00 » Digit Conversion Tree 2 Configuration

Digit Conversion Tree 2 Configuration

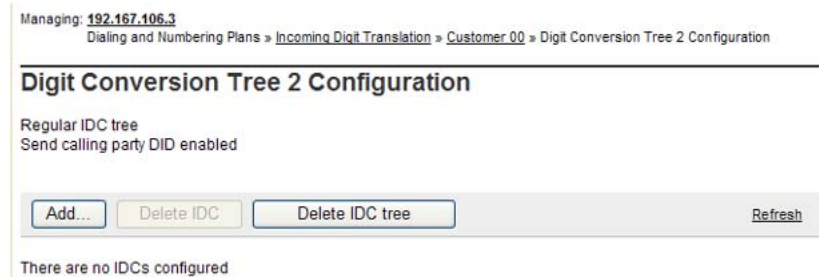
Type:

- ☒ Regular IDC tree
- ☒ Send calling party DID
- ☐ Flexible DID IDC tree

[Save](#) [Cancel](#)

Figure 19: Digit Conversion Tree Configuration

8. Click **Save**.
The Digit Conversion Tree Configuration page opens.



Managing: [192.167.106.3](#)
Dialing and Numbering Plans » Incoming Digit Translation » Customer 00 » Digit Conversion Tree 2 Configuration

Digit Conversion Tree 2 Configuration

Regular IDC tree
Send calling party DID enabled

[Add...](#) [Delete IDC](#) [Delete IDC tree](#) [Refresh](#)

There are no IDCs configured

Figure 20: Add Digit Conversion Tree

9. Click **Add**.
The Add Incoming Digits page opens.

Managing: 192.167.106.3
Dialing and Numbering Plans » Incoming Digit Translation » Customer 00 » Digit Conversion Tree 0 Configuration » Edit Incoming Digits

Edit Incoming Digits

Incoming Digits: 4681
Converted digits: 8884681 * (0 - 99999999)
CPND language:
☒ Roman characters
CPND Name:
first name, last name
Expected length: 13
Display format: First name, Last name ▾
☐ Katakana characters
CPND Name:
first name, last name
Expected length: ▾
Display format: First name, Last name ▾

Figure 21: Edit Incoming Digits

- 10. Enter the DID DN **Incoming Digits** to be converted.
 - 11. Enter the **Converted Digits = Mobility Prefix + DID DN**.
 - 12. Click **Save**.
- The Digit Conversion Tree Configuration opens.

Managing: 192.167.106.3
Dialing and Numbering Plans » Incoming Digit Translation » Customer 00 » Digit Conversion Tree 0 Configuration

Digit Conversion Tree 0 Configuration

Regular IDC tree
Send calling party DID disabled

	Incoming Digits	Converted Digits	CPND Name	CPND language
1 ○	4681	8884681		Roman characters

Figure 22: Digit Conversion Tree

Configuring a Handoff key

Use this procedure to configure the Handoff Key on an existing telephone in Element Manager.

-
1. Log on to Element Manager.
 2. In the navigation pane select **Phones**.
The Search for Phones pane opens.
 3. Click **Add**.
The New Phones page opens.
 - Enter Number of phones = 1
 - Choose Customer = 0
 - Choose Phone type = 2004P1 - IP Phone 2004P1 (example)
 4. Click **Preview**.
The Phone Details page opens.
 - Choose Customer Number = 0
 - Enter Terminal Number = 252 00 01 01 (example)
 - Enter Designation = SvcDN (example)
 - Enter Zone = 5 (example)

Note: Do not use the VTRK Zone. Virtual Trunks must be configured with a different zone number than the endpoints. This Zone = MO.
 5. Choose Key 1 = Key Type HNDO - Handoff.
 6. Click **Validate**. Check for Validation errors.
 7. Click **Finish**.
-

Configuring a HOT P key

Use this procedure to configure the HOT P Key in Element Manager.

-
1. Log on to Element Manager.
 2. In the navigation pane select **Phones**.
The Search for Phones pane opens.
 3. Click **Add**.
The New Phones page opens.
 - Enter Number of phones = 1
 - Choose Customer = 0

- Choose Phone type = UEXT - Universal Extension
4. Click **Preview**.

The Phone Details page opens.

- Choose Customer Number = 0
- Enter Terminal Number = 252 00 01 02 (example)
- Enter Designation = UEXT (example)
- Enter Zone = 5 (example)

Note: Do not use the VTRK Zone. Virtual Trunks must be configured with a different zone number than the endpoints. This Zone = MO.

5. Choose Key 00 = Prime DN, up to 7 digits.
 6. Choose Key 01 = 01 HOT P nn yyyzzzz, Mobility Prefix and extension to dial the Avaya 3100 MC - Client.
 7. Click **Validate**. Check for Validation errors.
 8. Click **Finish**.
-

Configuring the SIP trunk gateway

Configuring the SIP Trunk Gateway requires programming on both the Call Server and Signaling Server. The SIP Trunk Gateway can only be programmed with Element Manager.

Perform the following procedure to configure the Signaling Server.

-
1. Log on to Element Manager
 2. Select **System - IP Network - Nodes: Servers > Media Cards** from Element Manager navigator. The Node Configuration page opens.
 3. Click **Edit**.
 4. On the Edit page, select **Signaling Servers** to expand the section.
 5. Select the appropriate Signaling Server xxx.xxx.xxx.xxx properties. The properties for that Signaling Server appear.

Managing: 192.167.106.3
System » IP Network » Node Configuration » IP Telephony: Node ID 9 » Edit

Edit

Save and Transfer
Cancel

- + IP Telephony Node
- + VGW and IP phone codec profile
- + QoS
- + LAN configuration
- + SNTP
- + Virtual Trunk Network Health Monitor configuration
- + H323 GW Settings
- + Firmware
- + SIP GW Settings
- + SIP URI Map
- + SIP CD Services
- + SIP CTI Services
- + Microsoft Unified Messaging
- + Cards
- Signaling Servers
- Signaling Server 192.167.106.2

Add
Add
Remove

Properties

Role: Leader

Type: CPPM

Embedded LAN (ELAN) IP address: 192.167.106.2

Embedded LAN (ELAN) MAC address: 00:19:e1:e8:09:6f

Telephony LAN (TLAN) IP address: 192.167.107.2

Telephony LAN (TLAN) gateway IP address: 192.167.107.1

Hostname: cs1000ss

H323 ID: cs1000ss

Enable Line TPS: ☒

Enable IP Peer Gateway (Virtual Trunk TPS): SIP only

If Telephony LAN(TLAN) IP address and Telephony LAN(TLAN) gateway IP address are not in the same subnet as Telephony LAN (TLAN) Node IP address when Line TPS or IP Peer Gateway is enabled, then the TPS and/or VTRK applications will not run.

Enable SIP Proxy / Redirect Server: ☒

Local SIP TCP/UDP Port to Listen to: 5060

SIP Domain name: innlab.avaya.com

SIP Gateway Endpoint Name: cs1000ss

SIP Gateway Authentication Password: ••••••••

Enable Gatekeeper: ☐

Network Routing Service Role: Failsafe

Save and Transfer
Cancel

Figure 23: Signaling Server SIP

6. Select a SIP option from the **Enable IP Peer Gateway (Virtual Trunk TPS)** list.
7. Select **Enable SIP Proxy/Redirect Server**.
8. Verify the Local SIP Port.
This is the port to which the gateway listens. The default is 5060.
9. Type the **SIP Domain Name**.

The Domain name is case sensitive and must match the Service Domain name configured in the NRS.

10. If authentication is enabled in the NRS, configure the **SIP Gateway Endpoint Name** and **SIP Gateway Authentication Password** to match the Gateway Endpoint name and Gateway Endpoint authentication password used by the SIP Redirect Server.
 11. Click **Save and Transfer**.
-

Configuring the SIP Gateway settings

Perform the following procedure to configure the SIP Gateway settings.

-
1. Log on to Element Manager.
 2. Select **System - IP Network - Nodes: Servers > Media Cards** from the Element Manager navigator.
 3. On the Node Configuration page, click **Edit**.
 4. On the Edit page, select **SIP GW Settings** to expand the section.

Managing: [192.167.106.3](#)
System » IP Network » [Node Configuration](#) » IP Telephony: Node ID 9 » Edit

Edit

- + IP Telephony Node
- + VGW and IP phone codec profile
- + QoS
- + LAN configuration
- + SNTP
- + Virtual Trunk Network Health Monitor configuration
- + H323 GW Settings
- + Firmware
- SIP GW Settings
- TLS Security

Security Policy Security Disabled

TLS Security Port (1 - 65535)

Client Authentication ☐

Re-negotiation ☐

X.509 Certificate Authentication ☐

Primary Proxy or Re-direct Server

Primary Proxy or Redirect (TLAN) IP address

Port

Supports Registration ☒

Primary CDS Proxy or Re-direct server flag ☒

Transport Protocol UDP

Secondary Proxy or Re-direct Server

Figure 24: SIP Gateway settings

5. Complete the following for the primary server.

- **Primary Proxy or Re-direct (TLAN) IP address:** Enter the TLAN IP address of the server that hosts the NRS designated as the **Primary Re-direct Server**.
- **Supports Registration:** Select to have the SIP Gateway register with the Primary NRS.

Configuring the SIP URI to NPI/TON mapping

The SIP URI to NPI/TON mapping is used as a translation of a signaling request between the SIP Trunk Gateway and the NRS.

When using SIP, calls are routed based on SIP URLs instead of numbers. The SIP URI Map is used to identify the SIP domains to use for routing.

Use this procedure to configure the SIP URI Map settings in Element Manager.

1. Log on to Element Manager.
2. In the navigation pane click **System > IP Network > Node: Servers, Media Cards**. The Node Configuration page opens.
3. On the Node Configuration page, locate the node and click **Edit**.
4. Expand the **SIP URI Map** link.

Managing: 192.167.106.3

System » IP Network » Node Configuration » IP Telephony: Node ID 9 » Edit

Edit

- + IP Telephony Node
- + VGW and IP phone codec profile
- + QoS
- + LAN configuration
- + SNTP
- + Virtual Trunk Network Health Monitor configuration
- + H323 GW Settings
- + Firmware
- + SIP GW Settings
- SIP URI Map

Public E.164/National domain name	1	*
Public E.164/Subscriber domain name	1506	*
Public E.164/Unknown domain name	PublicUnknown	
Public E.164/Special Number domain name	PublicSpecial	
Private/UDP domain name	udp	
Private/CDP domain name	cdp.udp	
Private/Special Number domain name	PrivateSpecial	
Private/Unknown (vacant number routing) domain name	PrivateUnknown	
Unknown/Unknown domain name	UnknownUnknown	

Figure 25: SIP URI map
 Important:

The settings defined must be identical on each Call Server and the NRS.

- a. Enter **Public E.164/National domain name** = +1
- b. Enter **Public E.164/Subscriber domain name** = +1613
- c. Enter **Private/UDP domain name** = L1 Domain as defined in the NRS.
- d. Enter **Private/CDP domain name** = L0 domain.L1 domain as defined in the NRS.
- e. Click **Save and Transfer**.

Restarting the Signaling Server

There are two methods for restarting the Signaling Server:

Warm restart

- 1. From the EM navigator select **System > IP Network - Maintenance and Reports**
- 2. Select the node that contains the Signaling Server to be restarted.



Figure 26: Reset Signaling Server

Cold restart

Press the RST button on the faceplate of the Signaling Server.

Configuring NRS

The Network Routing Service (NRS) provides routing services to both SIP and H.323-compliant devices based on endpoints and routing stored in the active database. The database uses the information that the NRS extracted from the request to search its database.

For example, in the case of a SIP message or an H.323 ARQ message, the database attempts to find a registered endpoint that can terminate the call. The NRS Manager web server

interfaces with the database for viewing, adding, deleting, or modifying numbering plan configuration data and routing entries. All changes to the numbering plan database are carried out on the standby database. Changes that the administrator makes to the numbering plan database do not immediately affect call processing. The database must first be cut over to the active database by executing a database cut over command. The NRS database provides a central database of addresses that are required to route calls across the network.

The Avaya 3100 Mobile Communicator Gateway is defined as a Dynamic Gateway Endpoint on the Network Routing Server (NRS) SIP Proxy Server (SPS) and is assigned an endpoint name. Authentication is turned off. The endpoint name is configured on the Avaya 3100 Mobile Communicator Gateway as the gateway name under the list of gateway configuration parameters

NRS Database

The NRS database for each Network Routing Server has two schemas — an active schema and a standby schema.

- The active database is used for runtime location queries by SIP Proxy, Gatekeeper and Network Connection Service.
- The standby database is used by the administrator to modify the NRS database. An Administrator can only make changes to the standby database.

Committing NRS Database

When making changes to the standby database you must Cut over and Commit the database for the changes to become active.

1. In the navigation pane select **System > Database**.
The Database page opens.

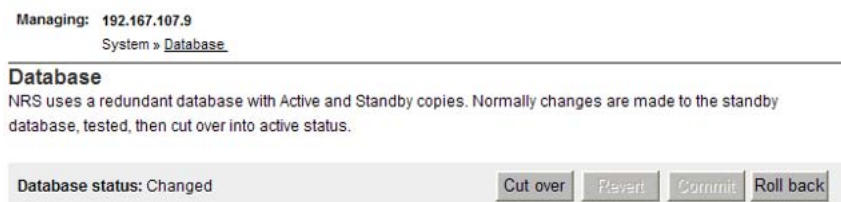


Figure 27: Database changed

2. Click **Cut over**.
The changed database becomes the active database.

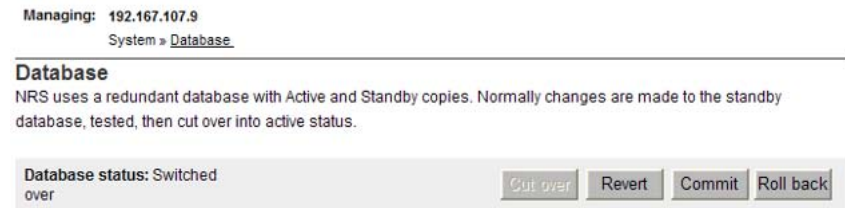


Figure 28: Database switched

3. Click the **Commit**.

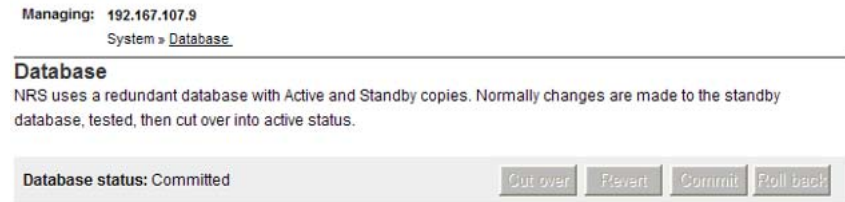


Figure 29: Database committed

The databases are synchronized. Both databases are changed.

Configuring Domain names on the NRS

Perform the following procedure to configure the Domain name on the Network Routing Service (NRS).

-
1. Open NRS Manager by doing one of the following: In ECM, select **Network > Elements** and then select the **NRS** from the Elements page.
OR
In Internet Explorer, enter the IP address of the NRS into the address bar.

Managing: 192.167.107.9
System » [NRS Server](#)

NRS Server

Service Status

Enable Graceful disable Restart

	Service Name	Service Status
1 ☐	SIP Proxy Server (SPS)	In service
2 ☐	Gatekeeper (GK)	In service
3 ☐	Network Connection Server (NCS)	In service

Server Configuration [Edit...](#)

NRS Setting

Host name cs1000nrs
Primary TLAN IP address 192.167.107.9
Secondary TLAN IP address 0.0.0.0

Figure 30: NRS Server

2. Click **Numbering Plans > Domains**.

Managing: ☐ Active database 192.167.107.9
☒ Standby database [Numbering Plan » Domains](#)

Domains

Domains establish the basic structure of your converged network, defined by Service domains, L1 (UDP) and L0 (CDP) domains.

Service Domains (1) L1 Domains (UDP) (1) L0 Domains (CDP) (1)

Add... Delete Refresh

ID	Description	# of L1 Domains	# of L0 Domains	# of Gateway Endpoints
1 ☐ innlab.avaya.com		1	1	2

Figure 31: Service Domains (1)

3. Ensure **Standby database** is selected.
The Standby database is used for administrator changes.
4. Ensure the required domain is available or click **Add** to add it.

Managing: ☐ Active database 192.167.107.9
☒ Standby database [Numbering Plan » Domains » Service Domains](#)

Edit Service Domain

Domain name: *

Domain description:

* Required value.

Save Cancel

Figure 32: Edit Service Domain

5. Ensure that the correct service domain, L1 domain, and L0 domain are available or **Add** them.

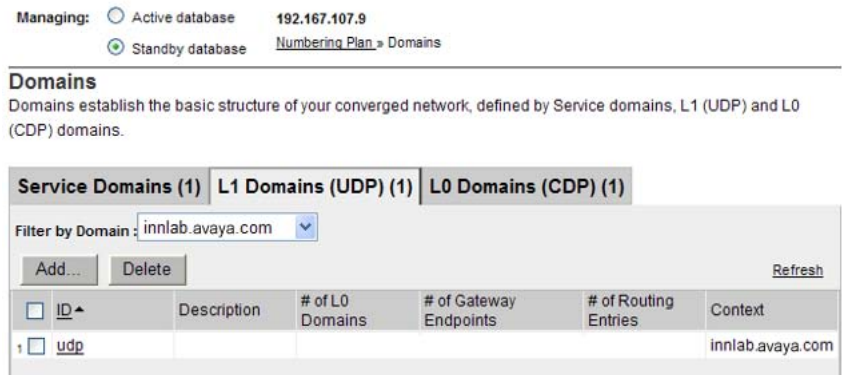


Figure 33: L1 Domains (UDP) (1)

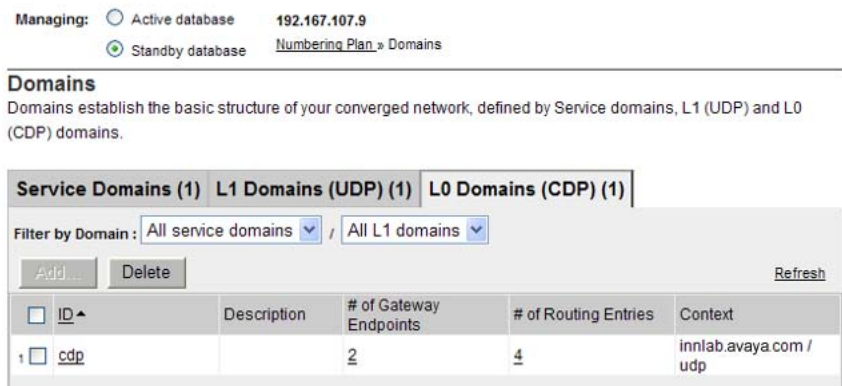


Figure 34: L0 Domains (CDP) (1)

6. Cut over and commit database, see [Committing NRS Database](#) on page 113.

 Note:

You need not cut over and commit the database, until after you complete all of the configuration procedures.

Configuring gateway endpoints on the NRS

Perform the following procedure to configure the gateway endpoints on the Network Routing Service (NRS). You must perform this procedure for each Avaya CS 1000 and Mobile Communicator Gateway node on the system.

On NRS redundant systems, perform all configuration on the primary NRS.

1. Open NRS Manager by doing one of the following: In Element Manager, select **Network, Elements** and select the NRS from the Elements page. OR In Internet Explorer, enter the IP address of the NRS into the address bar.
2. Ensure **Standby database** is selected.
The Standby database is used for administrator changes.
3. Click **Numbering Plans, Endpoints**. The search for Endpoints page appears.

Managing: ☐ Active database 192.167.107.9
☒ Standby database [Numbering Plan > Endpoints](#)

Search for Endpoints [Hide](#)

Enter an endpoint ID (use * for all) and click Search. You may narrow the search by specifying a particular domain.

Endpoint ID:

Limit results to Domain: / /

Results per page:

Gateway Endpoints (2) **User Endpoints (1)**

[Refresh](#)

☐ ID ▲	Supported Protocols	Call Signaling IP	Description	# of Routing Entries	Context
1 ☐ cs1000ss	Dynamic SIP endpoint	Not available		2	innlab.avaya.com / udp / cdp
2 ☐ mcq3100	Dynamic SIP endpoint	Not available		2	innlab.avaya.com / udp / cdp

Figure 35: Gateway Endpoints

4. Ensure that the correct domain, L1 domain, and L0 domain, and Gateway Endpoints are selected and click **Add**. The Add Gateway Endpoint Web page opens.

Managing: ☐ Active database 192.167.107.9
☒ Standby database [Numbering Plan](#) » [Endpoints](#) » [Gateway Endpoint](#)

Add Gateway Endpoint (innlab.avaya.com / udp / cdp)

End point name: *

Description:

Trust Node: ☒

Tandem gateway endpoint name: Not configured ▼

Endpoint authentication enabled: Authentication off ▼

Authentication password:

E.164 country code:

E.164 area code:

E.164 international dialing access code:

E.164 international dialing code length: (0-99)

E.164 national dialing access code:

E.164 national dialing code length: (0-99)

E.164 local (subscriber) dialing access code:

E.164 local (subscriber) dialing code length: (0-99)

Private L1 domain (UDP location) dialing access code:

Private L1 domain (UDP location) dialing code length: (0-99)

Private Special number 1:

Private Special number 1 dialing code length: (0-31)

Private Special number 2:

Private Special number 2 dialing code length: (0-31)

Static endpoint address type: IP version 4 ▼

Static endpoint address:

H.323 support: H.323 not supported ▼

SIP support: SIP not supported ▼

SIP TCP transport enabled: ☐

SIP TCP port: 5060

SIP UDP transport enabled: ☐

SIP UDP port: 5060

SIP TLS transport enabled: ☐

SIP TLS port: 5061

Persistent TCP support enabled ☒

End to end security support: ☐

Network Connection Server enabled: ☐

Redundancy enabled: Not Configured ▼

Main endpoint name: Not configured ▼

Redundant endpoint name: Not configured ▼

★ Required value

Save Cancel

Figure 36: Add Gateway Endpoint

5. For **Endpoint** name, type a relevant endpoint name.
 Example: 3100MCG
 Note: Endpoint names are case sensitive and must match.
6. Ensure that **Tandem Gateway Endpoint name** is blank.

7. Ensure that **Endpoint Authentication Enabled** is configured to **Authentication Off**.
 8. For **SIP support**, select **Dynamic SIP endpoint**.
 9. For **SIP transport**, select the transport protocol type. The Avaya 3100 Mobile Communicator supports UDP.
 10. Type a value for the **SIP port**, or leave the default value of 5060.
 11. Click **Save**.
 12. Cut over and commit database. See [Committing NRS Database](#) on page 113.
Note: It is not necessary to Cut over and commit the database until you have completed all the configuration procedures.
-

Adding a User Endpoint

Use this procedure to add a user endpoint to the NRS.

Each mobile client instance is represented by a User Endpoint (UE). Create the UE in the L0 domain that corresponds to the PBX that hosts the user. A typical UE attribute configuration is as follows:

- User name: user's Electronic Switched Network (ESN) number (for example, 3435335)
- Tandem gateway endpoint name: (do not configure) none
- L0 directory number (DN): a number based on the user's DN that can never match in the Coordinated Dialing Plan (CDP) or Universal Dialing Plan (UDP). This can be the last digit of the mobile prefix mobile prefix + User's ESN DN (for example, 53435335).
- L1 directory number (DN) prefix: (not required) none
- Authentication enabled: Authentication on
- Authentication password: xxxxxxxx

The Avaya 3100 Mobile Communicator Gateway registers as a gateway endpoint. As each client logs on, the Avaya 3100 Mobile Communicator Gateway uses the user account on the Avaya CS 1000 to validate the password of the user. Call routing does not use SIP registration.

1. Open NRS Manager by doing one of the following: In Element Manager, select **Network, Elements** and select the NRS from the Elements page. OR In Internet Explorer, enter the IP address of the NRS into the address bar.
2. Ensure **Standby database** is selected.
The Standby database is used for administrator changes.

The User Endpoints pane contains User Endpoints for (Service Domain / L1 Domain / L0 Domain).

3. Click **Numbering Plans, Endpoints**. The search for Endpoints page appears.

Managing: ☐ Active database 192.167.107.9
☒ Standby database [Numbering Plan » Endpoints](#)

Search for Endpoints [Hide](#)

Enter an endpoint ID (use * for all) and click Search. You may narrow the search by specifying a particular domain.

Endpoint ID:

Limit results to Domain: / /

Results per page:

Gateway Endpoints (2) | User Endpoints (0)

☐	ID	L0 DN	L1 DN Prefix	E.164 Local DN Prefix	E.164 Area Code	E.164 Country Code	Registration Status	Context

1 - 2 of 2 User Endpoint(s) Page 1 of 1 [First](#) [Previous](#) [Next](#) [Last](#)

Figure 37: Search User Endpoints

4. Ensure that the correct domain, L1 domain, and L0 domain, and Gateway Endpoints are selected and click **Add**. The Add User Endpoint Web page opens.

Managing: ☐ Active database 192.167.107.9
☒ Standby database [Numbering Plan » Endpoints » User Endpoint](#)

Add User Endpoint (innlab.avaya.com / udp / cdp)

User name: *

User endpoint description:

Trust Node: ☐

Tandem gateway endpoint name:

L0 directory number (DN): *

L1 directory number (DN) prefix:

E.164 local directory number (DN) prefix:

E.164 Area Code:

E.164 Country Code:

Authentication enabled:

Authentication password:

* Required value

Figure 38: Add User Endpoint

5. Complete the mandatory fields using the Job Aid.

6. Complete the optional fields as appropriate.
7. Click the **Save** button.
The standby database is updated. The Endpoints Web page opens, showing the newly added User Endpoint in the User Endpoints pane.
8. If required, click **Add** to add additional User Endpoints. The User Endpoints Web page displays any new endpoints.

Managing: ☐ Active database 192.167.107.9
☒ Standby database [Numbering Plan » Endpoints](#)

Search for Endpoints [Hide](#)

Enter an endpoint ID (use * for all) and click Search. You may narrow the search by specifying a particular domain.

Endpoint ID:

Limit results to Domain: / /

Results per page:

Gateway Endpoints (2) **User Endpoints (2)**

[Refresh](#)

	ID	L0 DN	L1 DN Prefix	E.164 Local DN Prefix	E.164 Area Code	E.164 Country Code	Registration Status	Context
1	4680	88474680		640	506	1	Not available	innlab.avaya.com / udp / cdp
2	4681	88474681		640	506	1	Not available	innlab.avaya.com / udp / cdp

1 - 2 of 2 User Endpoint(s) Page 1 of 1 [First](#) [Previous](#) [Next](#) [Last](#)

Figure 39: User Endpoints

 Important:

A maximum of 100 user endpoints can be displayed on the User Endpoints Web page.

 Important:

On login, the Avaya 3100 MC - Client users validate their password against the NRS; however they never will show as registered against the NRS. To view user status, refer to the User Info tab on the Avaya 3100 Mobile Communicator Gateway Web administration interface.

9. Cut over and commit database, see [Committing NRS Database](#) on page 113.
Note: It is not necessary to Cut over and commit the database until you have completed all the configuration procedures.

Job Aid

The following table to understand the Add User Endpoint Web page fields.

Field	Description
User name	Enter a User name for the endpoint. The endpoint's user name must be alphanumeric (a...z, A...Z, 0...9) and can be up to 30 characters in length. The user name, together with the Service Domain names, becomes a string that is used to build the user's SIP URI. Frequently, this field is configured with the user's extension number. Example 5340
User endpoint description	The endpoint's description can use most keyboard characters (except single quotes) and can be up to 120 characters in length. Frequently, this field is configured with the user's name. Example John Smith
Trust Node	The checkbox should be cleared.
Tandem gateway endpoint name	Configure the field to Not Configured .
L0 directory number (DN)	This field is a number that is based on the user's directory number. The number cannot match entries in the dial plan.
L1 directory number (DN) prefix	Leave as default.
E.164 local directory number (DN) prefix	Leave as default.
E.164 Area Code	Leave as default.
E.164 Country Code	Leave as default.
Authentication enabled	Select Authentication on from the drop-down list to enable authentication for this endpoint.
Authentication password	The password must be alphanumeric and can be up to 24 characters in length.

Adding an NRS Routing rule for the Avaya 3100 Mobile Communicator Gateway

Use this procedure to create an NRS Routing rule to route calls to the Avaya 3100 Mobile Communicator Gateway using the Mobility Prefix.

1. Open NRS Manager by doing one of the following: In Element Manager, select **Network, Elements** and select the NRS from the Elements page. OR In Internet Explorer, enter the IP address of the NRS into the address bar.
2. Ensure **Standby database** is selected.
The Standby database is used for administrator changes.
3. Select **Routes**.
The Routing Entries for (Service Domain / L1 Domain / L0 Domain / Endpoint) pane appears.
4. Select a Service Domain, an L1 Domain an L0 Domain and an Endpoint Name from the respective drop-down lists.
Note: Select the Avaya 3100 Mobile Communicator Gateway endpoint name.

Managing: ☐ Active database 192.167.107.9
☒ Standby database [Numbering Plan](#) » Routes

Search for Routing Entries [Hide](#)

Enter a DnPrefix and Dn Type (use * for all) and click Search. You may narrow the search by specifying a particular domain.

DN Prefix: DN Type:

Limit results to Domain: / /

Endpoint Name:

Results per page:

Routing Entries (0) **Default Routes (0)**

☐	DN Prefix	DN Type	Route Cost	SIP URI Phone Context	Context

1 - 1 of 1 Routing Entry(ies) Page 1 of 1 First| Previous| Next| Last

Figure 40: Search for Routing Entries MGC 3100

5. Ensure that the correct Domain, L1 domain, L0 domain, Endpoint Name and the Routing Entries tab are selected and click Add. The Add Routing Entry page opens.
Note: Select Private level 0 regional (CDP steering code). Enter the Mobility Prefix for the DN prefix.

Managing: ☐ Active database 192.167.107.9
☒ Standby database [Numbering Plan > Routes > Routing Entry](#)

Add Routing Entry (innlab.avaya.com / udp / cdp / 3100mcg)

DN type: Private level 0 regional (CDP steering code) ▼

DN prefix: 888 *

Route cost: 1 * (1-255)

* Required value.

Save Cancel

Figure 41: Adding routing entry MGC 3100

6. Click Save.
- The standby database is updated. The Routes web page opens, displaying the newly added routing entry in the Routing Entries pane.
7. Ensure your Routing Entries page displays the Mobility Prefix (888) for the DN Prefix and has the 3100 MCG Endpoint Name (3100mcg) in the Context field.

Managing: ☐ Active database 192.167.107.9
☒ Standby database [Numbering Plan > Routes](#)

Search for Routing Entries Hide

Enter a DnPrefix and Dn Type (use * for all) and click Search.You may narrow the search by specifying a particular domain.

DN Prefix: * DN Type: All DN Types ▼

Limit results to Domain: innlab.avaya.com ▼ / udp ▼ / cdp ▼

Endpoint Name: 3100mcg ▼

Results per page: 50 ▼ Search

Routing Entries (1) Default Routes (0)

Add... Copy... Move... Routing test... Delete Export Import Refresh

☐	DN Prefix ▲	DN Type	Route Cost	SIP URI Phone Context	Context
1 ☐	888	Private level 0 regional (CDP steering code)	1	cdp.udp	innlab.avaya.com/ udp / cdp / mcg3100

1 - 1 of 1 Routing Entry(ies) Page 1 of 1 First| Previous| Next| Last

Figure 42: Routing entry mobility prefix

8. Cut over and commit database, see [Committing NRS Database](#) on page 113.
- Note: It is not necessary to Cut over and commit the database until you have completed all the configuration procedures.

Adding an NRS Routing rule for the Avaya CS 1000

Use this procedure to create an NRS Routing rule to route calls to the Avaya CS 1000.

1. Open NRS Manager by doing one of the following: In Element Manager, select **Network, Elements** and select the NRS from the Elements page. OR In Internet Explorer, enter the IP address of the NRS into the address bar.
2. Ensure **Standby database** is selected.
The Standby database is used for administrator changes.
The User Endpoints pane contains User Endpoints for (Service Domain / L1 Domain / L0 Domain).
3. Select **Routes**,
The Routing Entries for (Service Domain / L1 Domain / L0 Domain / Endpoint) pane appears.
4. Select a Service Domain, an L1 Domain an L0 Domain and an Endpoint Name from the respective drop-down lists.
Note: Select the Avaya CS 1000 (cs1000ss) endpoint name.

Managing: ☐ Active database 192.167.107.9
☒ Standby database [Numbering Plan > Routes](#)

Search for Routing Entries [Hide](#)

Enter a DnPrefix and Dn Type (use * for all) and click Search. You may narrow the search by specifying a particular domain.

DN Prefix: DN Type:

Limit results to Domain: / /

Endpoint Name:

Results per page:

Routing Entries (0) **Default Routes (0)**

☐ DN Prefix	DN Type	Route Cost	SIP URI Phone Context	Context

1 - 1 of 1 Routing Entry(ies) Page 1 of 1 First| Previous| Next| Last

Figure 43: Search for Routing Entries Avaya CS 1000

5. Ensure that the correct Domain, L1 domain, L0 domain, Endpoint Name and the Routing Entries tab are selected and click Add. The Add Routing Entry page opens.
Note: Select Private level 0 regional (CDP steering code). Enter the digits necessary to steer calls to the number block of the DID DNs used by the Avaya 3100 Mobile

Communicator. In the example 46 is used to capture the DID DN numbers 4680-4689.

Managing: ☐ Active database 192.167.107.9
☒ Standby database [Numbering Plan » Routes » Routing Entry](#)

Add Routing Entry (innlab.avaya.com / udp / cdp / cs1000ss)

DN type: Private level 0 regional (CDP steering code) ▼

DN prefix: 46 *

Route cost: 1 * (1-255)

* Required value.

Save Cancel

Figure 44: Add routing entry Avaya CS 1000

6. Click **Save**.
The standby database is updated. The Routes web page opens, displaying the newly added routing entry in the Routing Entries pane.
7. Ensure your Routing Entries page displays the DN Prefix with the leading digits for the DID DNs DN Prefix and has the CS 1000 Endpoint Name (cs1000ss) in the Context field.

Managing: ☐ Active database 192.167.107.9
☒ Standby database [Numbering Plan » Routes](#)

Search for Routing Entries [Hide](#)

Enter a DnPrefix and Dn Type (use * for all) and click Search.You may narrow the search by specifying a particular domain.

DN Prefix: * DN Type: All DN Types ▼

Limit results to Domain: innlab.avaya.com ▼ / udp ▼ / cdp ▼

Endpoint Name: cs1000ss ▼

Results per page: 50 ▼ Search

Routing Entries (1) Default Routes (0)

Add... Copy... Move... Routing test... Delete Export Import Refresh

☐ DN Prefix ▲	DN Type	Route Cost	SIP URI Phone Context	Context
☒ 46	Private level 0 regional (CDP steering code)	1	cdp.udp	innlab.avaya.com / udp / cdp / cs1000ss

1 - 1 of 1 Routing Entry(ies) Page 1 of 1 First| Previous| Next| Last

Figure 45: Routing entry Avaya CS 1000

8. Cut over and commit database, see [Committing NRS Database](#) on page 113.
Note: It is not necessary to Cut over and commit the database until you have completed all the configuration procedures.

Chapter 12: CallPilot MWI configuration

This section describes the Call Pilot Message Waiting Indication (MWI) configuration for Avaya CS 1000 and Avaya CS 2100.

MWI for Avaya CS 1000

For CallPilot to send message waiting indicator (MWI) notifications to the mobile clients, you must configure CallPilot with an alternate DN against the primary DN for the user. The alternate DN must be equal to the UEXT target DN used to extend SIP calls to the mobile clients. The format is:

<mobility prefix><Avaya 3100 MC - Client username>

Example: 888881234567

When CallPilot sends the Message Waiting Indicator (MWI) notification, the following series of events occurs:

1. CallPilot sends the notification to the Avaya CS 1000.
2. The Avaya CS 1000 sends the notification (an unsolicited SIP message) to the SPS and on to the Avaya 3100 Mobile Communicator Gateway.
3. The Avaya 3100 Mobile Communicator Gateway sends the MWI notification using HTTP or HTTPS over the cellular data channel to the mobile client.



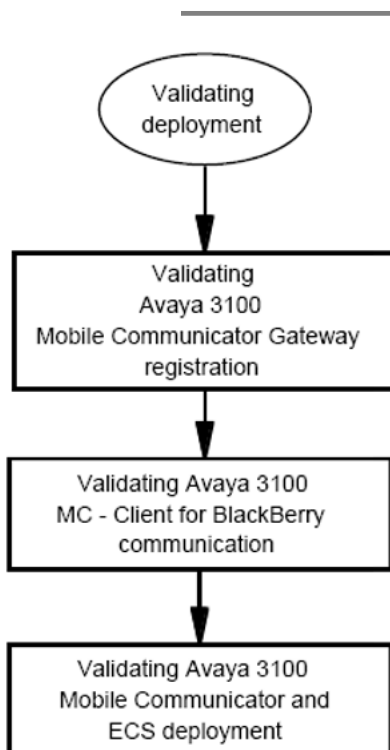
Important:

To support MWI for Avaya 3100 Mobile Communicator, you must enable the Premium Service and NMS packages (175, 219). Refer to CallPilot documentation for details on when these packages are required to be determined for your specific configuration.

Chapter 13: Validate deployment

This section describes how to validate that the Avaya 3100 Mobile Communicator components and the Avaya Communication Server 2100 (Avaya CS 2100) Enterprise Call Server (ECS) integration is correct.

Validating deployment task flow



Validating deployment task flow navigation

- [Validating Avaya 3100 Mobile Communicator Gateway registration](#) on page 130
- [Validating Avaya 3100 MC - Client for BlackBerry communication](#) on page 131
- [Validating Avaya 3100 Mobile Communicator and Avaya CS 1000 ECS deployment](#) on page 132

Validating Avaya 3100 Mobile Communicator Gateway registration

Use this procedure to determine if the Avaya 3100 Mobile Communicator Gateway is registered to the Enterprise Communication Server (ECS).

Prerequisites

The Service Number for the trunk between the Avaya 3100 Mobile Communicator Gateway and the SIP PBX interface is configured on the Avaya Communication Server 2100 (Avaya CS 2100) ECS, and matches the entered Service Number information in the Avaya 3100 Mobile Communicator Gateway.

-
1. Log in to the Avaya 3100 Mobile Communicator Gateway through the Admin Login page.
 2. On the **System Status** tab, check for the presence of alarms under the **Last Alarm Entry** column.
 3. If an alarm entry exists, click on the link to view the alarm details. If the alarm details indicate a registration failure, the Avaya 3100 Mobile Communicator Gateway is not currently registered. Check your configuration and try again.

See the [Job aid](#) on page 130 following this procedure for an example of successful and unsuccessful registration attempts.

Job aid

The following figure shows a successful registration attempt with no alarms.

System Status							
System Status							
Gateway Servers							
IP Address	Domain Name	Status	Last Alarm Entry	Active Connections	Queued Messages	System Load	Tx (kbps)
192.167.130.75	3100mcg.inlab.avaya.com		No Alarms	0	0	0.00	0.00
License Used/Limit		Single: 2/30					

Figure 46: Successful registration

The following figure shows an unsuccessful registration attempt with an alarm entry.

System Status								
System Status								
Gateway Servers								
IP Address	Domain Name	Status	Last Alarm Entry	Active Connections	Queued Messages	System Load	Tx(kbps)	Rx(kbps)
47.10.10.10	iotmcg3100.extiot.com	Running	06/17/2009 16:06:37 (1)	1	0	0.00	0.00	0.00
License Used/Limit		Single: 9/20						

Figure 47: Unsuccessful registration

The following figure shows an unsuccessful registration attempt with the alarm entry details.

System Status										Logout / Help												
System Status		System Configuration		Device Configuration		User Info		Instant Conferencing		Tools	Admin Portal											
System Status																						
Gateway Servers																						
IP Address		Domain Name		Alarm for: 47.230.77.187								Tx(kbps)		Rx(kbps)								
47.10.10.10		iotmcg3100.extiot.com										0.00		0.00								
License Used/Limit																						
		<table><thead><tr><th>Level</th><th>Component</th><th>Type</th><th>Message</th><th>Date</th></tr></thead><tbody><tr><td>SEVERE</td><td>Call DID Registration</td><td>OutgoingCallDIDRegistrationFailed</td><td>Outgoing call DID registration failed.</td><td>Wed Jun 17 16:06:37 GMT-500 2009</td></tr></tbody></table>											Level	Component	Type	Message	Date	SEVERE	Call DID Registration	OutgoingCallDIDRegistrationFailed	Outgoing call DID registration failed.	Wed Jun 17 16:06:37 GMT-500 2009
Level	Component	Type	Message	Date																		
SEVERE	Call DID Registration	OutgoingCallDIDRegistrationFailed	Outgoing call DID registration failed.	Wed Jun 17 16:06:37 GMT-500 2009																		
		Download alarm logs																				
		Close																				

Figure 48: Alarm entry details

Validating Avaya 3100 MC - Client for BlackBerry communication

Use this procedure to ensure that you can connect to the Avaya 3100 Mobile Communicator Gateway through the BlackBerry Enterprise Server (BES).

1. On your BlackBerry mobile client, open the BlackBerry Mobile browser.
2. Navigate to the User Portal of the Avaya 3100 Mobile Communicator Gateway server (<http://<hostname>:8282/adminserver/userportal.html>).

If you can view the Avaya 3100 Mobile Communicator Gateway User Portal, then you have proper communication between the client and the Avaya 3100 Mobile Communicator Gateway servers.

Validating Avaya 3100 Mobile Communicator and Avaya CS 1000 ECS deployment

This procedure tests a number of scenarios, in increasing order of complexity, to ensure that the configuration of the Avaya 3100 Mobile Communicator Gateway, Avaya 3100 Mobile Communicator - Client (Avaya 3100 MC - Client), Avaya Communication Server 2100 (Avaya CS 2100) ECS, and Lightweight Directory Access Protocol (LDAP) server interact correctly.

Prerequisites

- Avaya 3100 Mobile Communicator Gateway is installed and configured.
- Avaya 3100 MC - Client is installed and configured on a number of devices.
- Avaya Communication Server 2100 (Avaya CS 2100) ECS is configured to support Avaya 3100 Mobile Communicator.
- LDAP server is accessible.

Refer to the following user guides for configuration instructions:

- *Avaya 3100 Mobile Communicator - Client for Blackberry User Guide, NN42030-101*
- *Avaya 3100 Mobile Communicator - Client for Nokia User Guide, NN42030-102*
- *Avaya 3100 Mobile Communicator - Client for Windows Mobile User Guide, NN42030-107*
- *Avaya 3100 Mobile Communicator - Client for iPhone User Guide, NN42030-111*

-
1. Configure the Avaya 3100 Mobile Communicator Gateway to not require encryption.
 2. Configure the Avaya 3100 MC - Client for BlackBerry to not require encryption.
 3. Log in to the Avaya 3100 MC - Client for BlackBerry (uses HTTP).
Validates that the Avaya 3100 MC - Client can register with the Avaya 3100 Mobile Communicator Gateway and SPS.
 4. Configure the Avaya 3100 MC - Client for Nokia or Avaya 3100 MC - Client for Windows Mobile to not require encryption.
 5. Log in to the Avaya 3100 MC - Client for Nokia or Avaya 3100 MC - Client for Windows Mobile (uses HTTP).
Validates that the Avaya 3100 MC - Client can register with the Avaya 3100 Mobile Communicator Gateway and Avaya CS 1000ECS.

6. Configure one of the clients to require encryption. Use this client in the remainder of this procedure.
 7. Log in to the client using HTTPS.
Validates that certificates are functioning correctly.
 8. Dial the mobile device from another telephone.
 9. Accept the call using the Avaya 3100 MC - Client.
Tests that the setup (MADN, Simring, etc.) for incoming calls, the Call Server dial plan, and the routing are configured correctly.
 10. Make a Call-me-first call from the client.
Tests that the setup for incoming calls, the Call Server dial plan, and the routing are configured correctly.
 11. Make a direct outbound call from the client.
Validates that the service DN routing to the Avaya 3100 Mobile Communicator Gateway is correct.
 12. Test mid-call features on the client (for example, hold and retrieve, transfer, or conference).
Verifies DTMF handling and more complex call scenarios.
 13. Perform a corporate directory search from the client for a known user.
Verifies that the LDAP to Avaya 3100 Mobile Communicator Gateway connections and data mapping are correct.
 14. Add a user from the corporate directory search to the buddy list.
 15. Send an instant message to the added user.
Validates the LDAP field mapping and instant message functionality.
 16. Check that you can see the presence status of the user.
Validates the LDAP field mapping and presence.
-

Validate deployment

Chapter 14: Upgrade fundamentals

This chapter describes the following upgrade paths:

- Release 2.x to Release 3.0 upgrade
- Release 3.0 to Release 3.1 upgrade
- Service Upissue upgrade
- Converting to a redundant configuration



Important:

Use the server system console for installations and upgrades. Do not use a remote terminal.



Warning:

During upgrades, users are logged out of the server being upgraded and redirected to the standby system (if available). Schedule the upgrade during off-peak hours to minimize user impact.

In redundant systems, you upgrade one server and return it to service before upgrading the second server. Where possible, do not change the way that users access the system (for example, the IP address or Fully Qualified Domain Name).

When the mobile client applications require updating, you should instruct your users to record their login configuration, so that they can restore their configuration after the upgrade completes.

If the initial installation is a standalone configuration you can convert to a redundant configuration.

Navigation

- [Upgrade work flow](#) on page 136
- [Upgrading from Release 2.x to Release 3.0](#) on page 136
- [Upgrading from Release 3.0 to Release 3.1](#) on page 139
- [Upgrading for a Service Upissue](#) on page 147
- [Converting to a redundant configuration](#) on page 148

Upgrade work flow

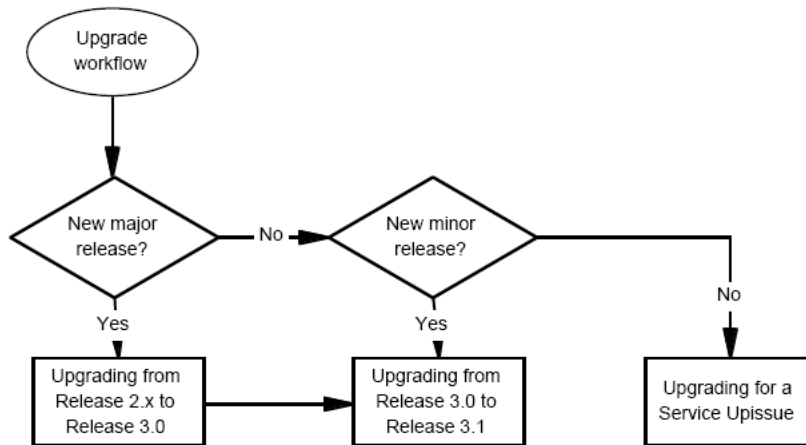


Figure 49: Upgrade workflow

Workflow navigation

- [Upgrading from Release 2.x to Release 3.0](#) on page 136
- [Upgrading from Release 3.0 to Release 3.1](#) on page 139
- [Upgrading for a Service Upissue](#) on page 147

Upgrading from Release 2.x to Release 3.0

This section describes the tasks to upgrade the Avaya 3100 Mobile Communicator Gateway from Release 2.x to Release 3.0.

! Important:

Avaya 3100 Mobile Communicator Release 2.x cannot be directly upgraded to Release 3.1. You must upgrade to Release 3.0 using the Release 3.0 CD and the steps described in [Release upgrade taskflow](#) on page 137. After the upgrade, you upgrade from Release 3.0 to Release 3.1; see [Upgrading from Release 3.0 to Release 3.1](#) on page 139.

**Important:**

You must upgrade both Avaya 3100 Mobile Communicator Gateway servers at the same time, and the IP addresses must not change. The client upgrades require unchanged gateway server addresses.

Release upgrade taskflow

[Figure 50: Release upgrade task flow](#) on page 137 shows the upgrade tasks.

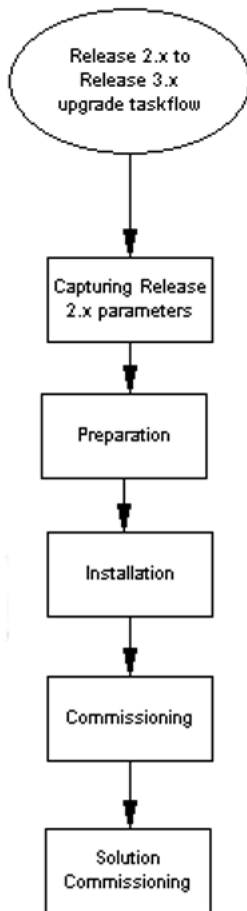


Figure 50: Release upgrade task flow

Release upgrade task flow navigation

- [Capturing Release 2.x parameters](#) on page 138
- [Preparation](#) on page 65
- [Installation](#) on page 72

- [Commissioning](#) on page 74
- [Solution commissioning](#) on page 92

**Important:**

When following the commissioning procedures for a Release 2.x to Release 3.0 upgrade, use the worksheet created in the upgrade task flow to guide the configuration steps.

[Table 13: Release 2.x to Release 3.0 upgrade times](#) on page 138 shows the times for completing each of the above procedures.

Table 13: Release 2.x to Release 3.0 upgrade times

Workflow	Time to complete task
Capturing Release 2.x parameters	10 minutes
Preparation	25 minutes per server
Installation	15 minutes per server
Commissioning	20 minutes
Solution commissioning	4 hours, plus 20 minutes per user

Capturing Release 2.x parameters

Use this procedure to record the configuration of the Avaya 3100 Mobile Communicator Release 2.x system before upgrading the system to Release 3.0.

-
1. Access the Release 2.x Avaya 3100 Mobile Communicator Web Console, as described in the Release 2.x documentation suite.
 2. Click **Gateways**.
 3. Click **Configuration** for the Gateway.
 4. Fill in [Job Aid: Release 2.x parameter worksheet](#) on page 139.
 5. Log out of the Web Console.
-

Job Aid: Release 2.x parameter worksheet

Fill in the following worksheet with the values from your Release 2.x system. Use the values when you commission your Release 3.0 system.

Release 2.x parameter	Corresponding Release 3.0 parameter	Contents
Gateway Address	Server Address	
Backup Gateway SIP Listening Address	Server Address (of the backup Avaya 3100 Mobile Communicator Gateway)	
Gateway SIP Listening Address	SIP Port	
Primary (ECS) Address	Primary ECS Address	
Secondary ECS Address	Secondary ECS Address	
Group Call Server Address	Media Server	
LDAP Server Address	URL	
LDAP Username	LDAP Username	
LDAP Password	Password	
LDAP Search Base	Search Base	
LDAP Security Authorization	Authorization	
Gateway Name	Gateway Name	
User Prefix for Call Termination	User Prefix for Call Termination	
User Prefix/Phone-context for Call Origination	User Prefix/Phone-context for Call Origination	
Dial In Service DN	Dial In Service DN	
Domain	Domain	

Upgrading from Release 3.0 to Release 3.1

This section describes the tasks to upgrade the Avaya 3100 Mobile Communicator Gateway from Release 3.0 to Release 3.1.

**Important:**

Upgrade one Avaya 3100 Mobile Communicator Gateway server and return it to service before upgrading the other server. As soon as you start the upgrade on the active system, the redundant server becomes the active server.

Prerequisites

Ensure that you have copies of the license file and any CA certificates backed up to a known location (for example, on the server disk in a folder in /tmp) before you start the upgrade procedure.

Upgrading from Release 3.0 to Release 3.1 taskflow

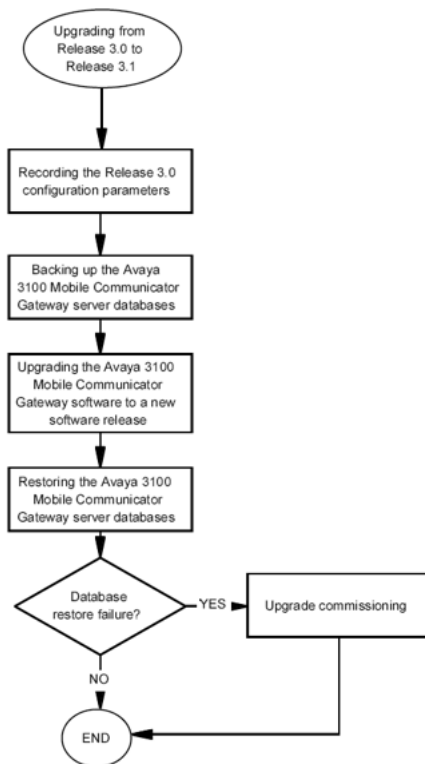


Figure 51: Upgrading from Release 3.0 to Release 3.1 task flow

Upgrading from Release 3.0 to Release 3.1 task flow navigation

- (optional) [Recording the Release 3.0 configuration parameters](#) on page 141

- [Backing up the Avaya 3100 Mobile Communicator Gateway server databases](#) on page 160
 - [Upgrading the Avaya 3100 Mobile Communicator Gateway software to a new software release](#) on page 145
 - (optional) [Restoring the Avaya 3100 Mobile Communicator Gateway server databases](#) on page 161
 - (optional) If the database restore fails, follow [Upgrade commissioning](#) on page 147
-

Recording the Release 3.0 configuration parameters

Use this procedure to record all the Release 3.0 configuration parameters, in the unlikely case that your database restore fails.

Prerequisites

- You must be logged into the Avaya 3100 Mobile Communicator Web Administration Console as administrator. For more information, see [Logging on to the Avaya 3100 Mobile Communicator Web Administration Console as an administrator](#).
- Have on hand a copy of the [Avaya 3100 Mobile Communicator Gateway worksheet](#) on page 164. For more information, see [Release 3.0 system configuration job aid](#) on page 142.

-
1. Click the **System Configuration** tab.
 2. Select **Gateway Actions, Configure Gateway**.
 3. In redundant configurations, select the gateway.
 4. Click **Edit**.
 5. Record the gateway configuration parameters in the Avaya 3100 Mobile Communicator Gateway worksheet.
 6. Click **Close**.
 7. In redundant systems, repeat steps 2 through 6 for the second gateway.
 8. Click the **Device Configuration** tab.
 9. Click **Edit**.
 10. In [Table 15: Device settings configuration](#) on page 144, record the Device configuration.

11. Click the **Tools** tab.
12. In [Table 16: Tools configuration](#) on page 145, record the Tools configuration.

Release 3.0 system configuration job aid

Use the following tables to record your system configuration. Parameters that are not used in Release 3.1, or do not exist in Release 3.0, do not appear in these tables.

- [Table 14: Gateway settings configuration](#) on page 142
- [Table 15: Device settings configuration](#) on page 144
- [Table 16: Tools configuration](#) on page 145

Table 14: Gateway settings configuration

Section	Release 3.0 field name	Release 3.1 field name	Server 1 configuration	Server 2 configuration
Mobility Server	Server Address	Server Address		
	SIP Port	SIP Port		
	Domain	Domain		
	Gateway name	Gateway name		
	Incoming Call Reliable Timer	Incoming Call Reliable Timer		
	Primary ECS Address	Primary ECS Address		
	Secondary ECS Address	Secondary ECS Address		
Device Access	HTTP Port	HTTP Port		
	HTTPS Port	HTTPS Port		
	HTTPS certificate password	HTTPS certificate password		
Dial Plan	User Prefix/ Phone-context for Call Origination	User Prefix/ Phone-context for Call Origination		
	User Prefix for Call Termination	Mobility Prefix		

Section	Release 3.0 field name	Release 3.1 field name	Server 1 configuration	Server 2 configuration
	Dial-In Service DN	Dial-In Service DN		
	Dialplan Conversion List	Dialplan Conversion List		
DTR	Initial port for DTR (27000-27499)	Initial port for DTR (27000-27499)		
	Mid-Call Cellular Prefix	Mid-Call Cellular Prefix		
LDAP	URL	URL		
	Search Base	Search Base		
	LDAP Username	LDAP Username		
	Authorization	Authorization		
	Password	Password		
	LDAP tag for user ID	LDAP attribute tag that contains the user id		
	LDAP tag for user first name	LDAP attribute tag that contains the user's first name		
	LDAP tag for user's last name	LDAP attribute tag that contains the user's last name		
	LDAP tag for user display name	LDAP attribute tag that contains the user's display name		
	LDAP tag for user business #	LDAP attribute tag that contains the user's business phone #		
	LDAP tag for user mobile #	LDAP attribute tag that contains the user's mobile phone #		

Section	Release 3.0 field name	Release 3.1 field name	Server 1 configuration	Server 2 configuration
	LDAP tag for user's email	LDAP attribute tag that contains the user's email address		
	LDAP tag for user extension	LDAP attribute tag that contains the user's home phone		

Table 15: Device settings configuration

Section	Release 3.0 field name	Release 3.1 field name	Configuration
(3.0) Primary MG (3.1) Primary Avaya 3100 Mobile Communicator Gateway	External: Address (IP/host:Port)	External: Address (IP/host:Port)	
	External: Use Secure Connection	External: Use Secure Connection	
	Internal: Address (IP/host:Port)	Internal: Address (IP/host:Port)	
	Internal: Use Secure Connection	Internal: Use Secure Connection	
(3.0) Secondary MG (3.1) Secondary Avaya 3100 Mobile Communicator Gateway	External: Address (IP/host:Port)	External: Address (IP/host:Port)	
	External: Use Secure Connection	External: Use Secure Connection	
	Internal: Address (IP/host:Port)	Internal: Address (IP/host:Port)	
	Internal: Use Secure Connection	Internal: Use Secure Connection	
Access Numbers	Voice Mail Number	Voice Mail Numbers	
	Service Number	Service Numbers	
Dial Plan	Corporate Prefix Number	Corporate Prefix Number	
	Local Prefix Number	Local Prefix Number	
	Long Distance Prefix Number	Long Distance Prefix Number	
	International Prefix Number	International Prefix Number	

Section	Release 3.0 field name	Release 3.1 field name	Configuration
	Native Dialing Numbers	Native Dialing Numbers	
Auto-Download of Device Configuration	Allow Client Override	Allow Client Override	

Table 16: Tools configuration

Section	Release 3.0 field name	Release 3.1 field name	Configuration
Admin Server Port Setting	Enable HTTP port		
	Enable HTTPS port		

Upgrading the Avaya 3100 Mobile Communicator Gateway software to a new software release

During the software upgrade, a number of prompts appear. You can either accept the default value or enter a new value at each prompt.

Prerequisites

- You must be logged into the server as nortel. For more information, see [Accessing the server command line as nortel](#) on page 159.
- You must know the root password to perform the following procedure.
- You require a compact disc (CD) that contains the Avaya 3100 Mobile Communicator software.

1. Send a notice to users, to advise them to log off from the Avaya 3100 Mobile Communicator clients.
2. At the server (host server), insert the Avaya 3100 Mobile Communicator Gateway software CD into the CD-ROM drive.
3. Enter the following command:
appinstall
The installation script prompts you for the root password.
4. Enter the root password.
5. At the prompt to remove the previous installation, enter **y**.
6. At the prompt, choose one of the following options:

- 1 to install the upgrade and delete the existing data.
 - 2 to install the upgrade and retain the existing.
7. Read the Avaya software license agreement.
 8. To agree to the license agreement, enter **YES**
The software installation proceeds.
Messages appear to show installation progress. After the installation completes, the configuration script starts automatically.
 9. If you retained the data from the previous installation, cancel the configuration script and go to [13](#) on page 146.
The installation uses the existing data from before the upgrade.
OR
If you deleted the data from the previous installation, go to [10](#) on page 146.
 10. At the prompt for the ethernet address, select the card that corresponds to the IP address of this Avaya 3100 Mobile Communicator Gateway server.
 11. At the prompt for the mode, do one of the following:
 - If the Avaya 3100 Mobile Communicator Gateway configuration is not redundant, select Standalone mode, and go to [13](#) on page 146.
 - If the Avaya 3100 Mobile Communicator Gateway configuration is redundant, select Active-Standby mode, and go to [12](#) on page 146.
 12. For Active-Standby mode, at the prompt, enter the following information:
 - Server name: the domain name (if defined) or the internal IP address of the primary Avaya 3100 Mobile Communicator Gateway. This value is the same for both the primary and secondary Avaya 3100 Mobile Communicator Gateway servers.
 - Cluster name: this value is not currently in use. Use the default value.
 - Partner IP address: the IP address of the other Avaya 3100 Mobile Communicator Gateway server.
 13. After the configuration script finishes (or you cancel it), if a message appears to notify you that some backup files are missing, or that the database backup does not exist, select **OK**.
These messages are for your information only. The fact that files are missing could indicate an underlying issue.
 14. Select the files to restore by leaving the X beside each file that you want to restore, and clearing the X for any file that you do not want to restore.
 15. Press **Enter** to confirm your choices and to complete the restore process.
 16. Remove the CD.
-

Upgrade commissioning

If the database restore fails, you need to recommission the system using the parameters saved in [Recording the Release 3.0 configuration parameters](#) on page 141.

Prerequisites

- You must be logged into the server as nortel. For more information, see [Accessing the server command line as nortel](#) on page 159.
- You must know the root password to perform the following procedure.
- You must have all the information recorded in the tables in [Release 3.0 system configuration job aid](#) on page 142.

Use the configuration parameters, which you captured in [Release 3.0 system configuration job aid](#) on page 142, to commission the Release 3.1 system by following the procedures in [Commissioning](#) on page 74.

Upgrading for a Service Upissue

This section describes the upgrade due to an Avaya 3100 Mobile Communicator Gateway Service Upissue (SU). SUs are downloaded from the Web using FTP, and a CD is not required. A Maintenance Release (MR) is similar to an SU, but the update is not generally available, and you require a CD.

Upgrading the Avaya 3100 Mobile Communicator system software from CD

Use this procedure to perform maintenance patches to the system from a CD. Do not use this procedure to perform upgrades from release to release.

Prerequisites

You must know the root password to perform the following procedure.

Follow the steps in [Installation](#) on page 72, selecting the upgrade option when prompted.

Converting to a redundant configuration

If the initial installation is a standalone configuration you can convert to a redundant configuration.



Important:

This procedure assumes that you are not performing an upgrade at the same time.

Prerequisites

- You have already configured the new server on the network.
- You have already installed the Avaya 3100 Mobile Communicator Gateway software on the secondary server and cancelled the configuration. For more information, see [Installing the Avaya 3100 Mobile Communicator Gateway software](#) on page 73.
- You are familiar with the procedure to log on to the Avaya 3100 Mobile Communicator Web Administration Console as administrator. For more information, see [Logging on to the Avaya 3100 Mobile Communicator Web Administration Console as an administrator](#).
- You are familiar with the procedure to configure device settings on the Device Configuration tab. For more information, see [Configuring the device settings](#) on page 83.
- You are familiar with the required security certificate tasks. For more information, see *Avaya 3100 Mobile Communicator Administration and Security, NN42030-600*.

-
1. Log on to the server that hosts the primary gateway, as root.
 2. Run the configuration script:
`/opt/MobilityGatewaybin/mgsetup.sh`
 3. At the Ethernet prompt, accept the current values for the network interface card.
 4. At the mode prompt, select **2 Active-Standby**.
 5. For Active-Standby mode, at the prompt, enter the following information:
 - Server name: the domain name (if defined) or the internal IP address of the primary Avaya 3100 Mobile Communicator Gateway. This value is the same for both the primary and secondary Avaya 3100 Mobile Communicator Gateway servers.
 - Cluster name: this value is not currently in use. Use the default value.
 - Partner IP address: the IP address of the other Avaya 3100 Mobile Communicator Gateway server.
 6. Select **Finish** to save the configuration.
 7. Log on to the server that hosts the secondary gateway, as root.

8. Run the configuration script:
`/opt/MobilityGatewaybin/mgsetup.sh`
 9. At the prompt for the ethernet address, select the card that corresponds to the IP address of this Avaya 3100 Mobile Communicator Gateway server.
 10. At the mode prompt, select **2 Active-Standby**.
 11. For Active-Standby mode, at the prompt, enter the following information:
 - Server name: the domain name (if defined) or the internal IP address of the primary Avaya 3100 Mobile Communicator Gateway. This value is the same for both the primary and secondary Avaya 3100 Mobile Communicator Gateway servers.
 - Cluster name: this value is not currently in use. Use the default value.
 - Partner IP address: the IP address of the other Avaya 3100 Mobile Communicator Gateway server.
 12. Select **Finish** to save the configuration.
 13. Log on to the Avaya 3100 Mobile Communicator Web Administration Console as administrator.
 14. Click the **System Configuration** tab.
 15. Click **Gateway Actions > Configure Gateway**.
 16. On the Configure Gateway page, configure the local gateway parameters.
On a redundant system, the secondary gateway configuration comes from the primary gateway configuration, and is automatic.
 17. Click **Save**.
 18. Click **Close**.
You receive a prompt to restart the server.
 19. To restart the system and apply the new settings, click **Yes**.
 20. Click the **Device Configuration** tab.
 21. Click **Edit**.
 22. Configure the parameters for the secondary gateway.
 23. Click **Save**.
The new device settings apply for the next successful logon by each user. On a redundant system, the gateways automatically share the device settings.
 24. Perform any required security certificate tasks.
-

Chapter 15: Maintenance

This chapter contains procedures used to maintain the software.

Navigation

- [Removing a Service Upissue](#) on page 151
- [Uninstalling the Avaya 3100 Mobile Communicator system software](#) on page 152

Removing a Service Upissue

This procedure removes a Service Upissue (SU) from the system.



Important:

To completely remove the Avaya 3100 Mobile Communicator software from the system, see [Uninstalling the Avaya 3100 Mobile Communicator system software](#) on page 152.

Prerequisites

You must be logged into the server as nortel. For more information, see [Accessing the server command line as nortel](#) on page 159.

-
1. To list the current patches and SUs in service, enter `pstat`.
The server responds with information about the SU status.
 2. In the list of patches, identify the patch to remove and its handle. This handle is the input for the `<Patch_Handle>` parameter in the next step.



Important:

The next step stops the Avaya 3100 Mobile Communicator Gateway.

3. To take a patch or SU out of service, enter `poos <Patch_Handle>`.
The server responds `Patch handle: 0 The application mobilitybase should be stopped before putting out of service this Service Update Do you want to continue? (Y/N) [N]?`

4. Enter `y`.
The RPM patch removal completes.
 5. Enter `su`
 6. At the prompt, enter `<root_password>`
 7. To complete the removal, enter `/opt/mobilitybase-3.0-101a/postunpatch.sh`
The server continues the removal, which ends with the message `Pre uninstall phase done. Post uninstall phase done. Updating iptables rules: [ OK ] .`
 8. Enter the following command
`pout <Patch_Handle>`
 9. To check the SU installation, enter `pstat`
The server responds with information about the SU status.
 10. Verify that the correct SU version displays in the server response.
-

Job Aid

Use the following table to help you understand the parameters.

Parameter	Description
<code><Patch_Handle></code>	The handle associated with the patch to be removed.
<code><root_password></code>	The superuser password for the server.

Uninstalling the Avaya 3100 Mobile Communicator system software

You uninstall the Avaya 3100 Mobile Communicator Gateway (Avaya 3100 Mobile Communicator Gateway) system software from the command line.



Important:

This procedure removes the Avaya 3100 Mobile Communicator Gateway software from the server. Use [Removing a Service Upissue](#) on page 151 to remove patches.

Prerequisites

You must be logged into the server as nortel. For more information, see [Accessing the server command line as nortel](#) on page 159.

To delete the software, enter the following command:

```
sudo rpm -e mobilitygw mobileclients eas_gcs_telephony  
eas_gcs_locale-en_US
```

The **rpm** command removes the software from the system.

Chapter 16: Common procedures

This chapter contains the following procedures:

- [Logging on to the Avaya 3100 Mobile Communicator Web Administration Console as an administrator](#)
- [Managing the server processes from the Web Administration Console](#) on page 157
- [Managing the server processes from the command line](#) on page 158
- [Accessing the server command line as nortel](#) on page 159
- [Accessing the server command line as superuser](#) on page 159
- [Backing up the Avaya 3100 Mobile Communicator Gateway server databases](#) on page 160
- [Restoring the Avaya 3100 Mobile Communicator Gateway server databases](#) on page 161

Logging on to the Avaya 3100 Mobile Communicator Web Administration Console as an administrator

Log on to the Avaya 3100 Mobile Communicator Web Administration Console as an administrator to manage the system, monitor the users, monitor Instant Conferencing, and manage the client server repository.



Important:

Wait two minutes after starting the Avaya 3100 Mobile Communicator Gateway before accessing the Avaya 3100 Mobile Communicator Web Administration Console.

Prerequisites

- You need the administrator user id and password to perform this procedure.
- Access the Avaya 3100 Mobile Communicator Web Administration Console using a web browser.



Important:

User names and passwords are case-sensitive.

-
1. In the **Address** field of your Web browser, enter
`http://<IP address | hostname>:8282/adminserver`

OR

`https://<IP address | hostname>:8553/adminserver`

2. In the **Username** field, type the user name.
3. In the **Password** field, type the admin password.

 Important:

Avaya recommends that you change the default administrator password. For more information, see [Changing the Avaya 3100 Mobile Communicator Web Administration Console password](#) on page 156.

4. Click **Sign In**.
5. Click a tab at the top of the Avaya 3100 Mobile Communicator Web Administration Console to view the corresponding page.

Variable definitions

Variable	Value
<IP address hostname>	The name of the Avaya 3100 Mobile Communicator Gateway server in fully qualified domain name (FQDN) format, or the IP address of the server.
user name	Default: admin
admin password	Default: password

Changing the Avaya 3100 Mobile Communicator Web Administration Console password

Change the Avaya 3100 Mobile Communicator Web Administration Console password from the default password.

Prerequisites

You must be logged into the Avaya 3100 Mobile Communicator Web Administration Console as administrator. For more information, see [Logging on to the Avaya 3100 Mobile Communicator Web Administration Console as an administrator](#) on page 155.

1. On the Avaya 3100 Mobile Communicator Web Administration Console main page, click the **Tools** tab.
2. In the **Admin Server Password** section, in the **Current Password** box, type the current password.

**Important:**

Passwords are case-sensitive.

3. In the **New Password** box, type a new password.
4. In the **Confirm New Password** box, retype the new password.
5. In the **Admin Server Password** section, click **Save**.

Variable definitions

Variable	Value
Current Password	Existing password. The default password for new servers is <i>password</i>
New password	New password for the Admin server. Secure passwords use a mix of letters, numbers and alphabetic characters and can be up to 19 characters in length.
Confirm New Password	New password for confirmation.

Managing the server processes from the Web Administration Console

Start, stop, and restart server processes from the Web Administration Console to start, stop, or restart the servers.

Prerequisites

You must be logged into the Avaya 3100 Mobile Communicator Web Administration Console as administrator. For more information, see [Logging on to the Avaya 3100 Mobile Communicator Web Administration Console as an administrator](#).

-
1. Click the **System Configuration** tab.

The Status field indicates which server is currently active. In a single-server system, this is always the local server.

- Running—The server is running. In redundant configuration, the server is the active server.
- Connecting—The server is trying to connect to the Avaya 3100 Mobile Communicator server.
- Network Error—Connectivity to the server has been lost.
- Stopped—The server is stopped.
- Running-Standby—The server is in standby mode in a redundant configuration.

2. To stop the server processes, click **Gateway Actions** beside the server to be stopped and click **Stop**.
 3. To start the server processes, click **Gateway Actions** beside the server to be started and click **Start**.
 4. To restart the server processes, click **Gateway Actions** beside the server to be restarted and click **Restart**.
-

Managing the server processes from the command line

Instead of using the Web Administration Console, you can use the Linux command line to check, start, stop, and restart server processes.

Prerequisites

You must be logged into the server as superuser. For more information, see [Accessing the server command line as superuser](#) on page 159.

-
1. To check the server processes, enter

```
appstart status
```

The system responds with the status of the server processes.

2. To start the server, enter

```
appstart start
```

3. To stop the server, enter
`appstart stop`
4. To restart the server, enter
`appstart restart`

 Important:

Some implementations of the Avaya 3100 Mobile Communicator Gateway do not include the restart command.

Accessing the server command line as nortel

Use this procedure to access the server command line as nortel.

Prerequisites

You require the password to the nortel userid on the server.

-
1. Use SSH to connect to the server.
 2. At the userid prompt, enter `nortel`
 3. At the password prompt, enter `<password>`
-

Variable definitions

Variable	Value
<code><password></code>	The password associated with the nortel userid. For information about the default nortel password, see <i>Linux Platform Base and Applications Installation and Commissioning</i> , NN43001-315.

Accessing the server command line as superuser

Use this procedure to access the server command line as root.

Prerequisites

- You require the password to the nortel userid on the server.
- You require the password to the superuser (root) userid on the server.

-
1. Use SSH to connect to the server.
 2. At the userid prompt, enter `nortel`
 3. At the password prompt, enter `<password>`
 4. To become the root user, enter `su root`
 5. At the prompt, enter `<root_password>`
-

Variable definitions

Variable	Value
<code><password></code>	The password associated with the nortel userid. For information about the default nortel password, see <i>Linux Platform Base and Applications Installation and Commissioning, NN43001-315</i> .
<code><root_password></code> >	The password associated with the superuser. For information about the default superuser password, see <i>Linux Platform Base and Applications Installation and Commissioning, NN43001-315</i> .

Backing up the Avaya 3100 Mobile Communicator Gateway server databases

Use this procedure to back up the databases and current system configuration. You should perform this procedure after each installation or upgrade, and after you change the system configuration. The backup is created on the server. You should also store the backup in a different location (for example, on another server).

**Important:**

This procedure does not back up the language packages.

Prerequisites

You must be logged into the server as nortel. For more information, see [Accessing the server command line as nortel](#) on page 159.

-
1. To verify that the backup directory exists, enter:

```
ls /admin/nortel/backup
```

You should see mobilitybase in the directory list.

2. To backup the current system configuration, enter:

```
sudo /opt/mobilitybase/backup.sh
```

The system creates the backup file /admin/nortel/backup/mobilitybase/mobilitybasebackup.tar

 Important:

Avaya recommends that this backup file be copied to another server or other media.

When preparing for an upgrade from Release 3.0 to Release 3.1, copy the backup file to the /tmp directory of the server.

Restoring the Avaya 3100 Mobile Communicator Gateway server databases

Use this procedure if you need to restore system parameters.

 Important:

Perform the database restore procedure during a period of low system use because the system is out of service for two or more minutes, depending on the size of the databases.

 Important:

This procedure does not restore the language packages.

Prerequisites

- You must be logged into the server as superuser. For more information, see [Accessing the server command line as superuser](#) on page 159.
- Obtain a copy of the backup file if not available on the system. The file must be in the /admin/nortel/backup directory and named mobilitybasebackup.tar.



Important:

This procedure does not restore the shared files for the Instant Conferences.

-
1. To stop the server processes, enter the following command:

```
appstart stop
```

2. To restore the backup, enter the following command:

```
/opt/mobilitybase/restore.sh
```

3. To start the server processes, enter the following command:

```
appstart start
```

Chapter 18: Appendix A: Installation worksheets and checklist

This section contains worksheets to capture the system information and a checklist to assist you during the installation of the Avaya 3100 Mobile Communicator system.

- [Linux base worksheet](#) on page 163
- [Avaya 3100 Mobile Communicator Gateway worksheet](#) on page 164
- [Avaya 3100 Mobile Communicator solution checklist](#) on page 166

Linux base worksheet

Use the following worksheet to capture required information during the Linux base installation.

Table 17: Avaya Communication Server 1000 Linux base (5.50.12) configuration parameters

Configuration parameter	Value	Notes
ELAN IP Address		Configure to unused IP ELAN NIC is not used when COTS is installed as Avaya 3100 Mobile Communicator Gateway.
ELAN Gateway IP Address		Configure to unused IP ELAN NIC is not used when COTS is installed as Avaya 3100 Mobile Communicator Gateway.
ELAN Netmask		Configure to a value consistent with previous responses.
Hostname		Required. Must be present in DNS
TLAN port Domain Name		Required
TLAN IP Address		Required
TLAN Gateway IP Address		Required
TLAN Netmask		Required
Timezone		For example: US/Eastern

Configuration parameter	Value	Notes
Primary DNS Server		Required
Secondary DNS Server		Optional
Tertiary DNS Server		Optional
Network Time Protocol (NTP) Clock Source		Optional—Can be internal clock on COTS or IP.

Avaya 3100 Mobile Communicator Gateway worksheet

Use the following worksheet to capture required information for the Avaya 3100 Mobile Communicator Gateway installation.

Table 18: Avaya 3100 Mobile Communicator Gateway configuration parameters

Configuration parameter	Value	Notes
Domain		On the Avaya 3100 Mobile Communicator Gateway system configuration page, the domain is the SIP domain configured on the NRS.
Gateway Name		This is the endpoint name configured on the NRS for the Avaya 3100 Mobile Communicator Gateway
Primary ECS Address		Primary NRS IP
Secondary ECS Address		Secondary NRS IP
User Prefix/Phone-context for Call Origination		This is the phone-context value configured on the NRS. If using a UDP number for the Avaya 3100 MC - Client user name, this is the UDP phone-context. If CDP, then use the CDP phone context.
User Prefix for Call Termination		This is the "Mobility HLOC", which is the prefix used on the hotp key of the UEXT calls to allow the NRS to route calls to the Avaya 3100 Mobile Communicator Gateway. The Avaya 3100 Mobile

Configuration parameter	Value	Notes
		Communicator Gateway strips this prefix for incoming calls to produce the user name of the Avaya 3100 MC - Client users. For example, if you configure 88888 as the Mobility HLOC, 888881234 is configured on the hotp key of a UEXT for DN 1234. Then when a call is extended to the Avaya 3100 Mobile Communicator Gateway by the UEXT, the Avaya 3100 Mobile Communicator Gateway strips the prefix 88888 to produce the username 1234.
Dial-In Service DN		On Avaya 3100 Mobile Communicator Gateway system configuration page this service DN is the format of the number incoming from the NRS (which will likely be different from the PSTN number depending on the dial plan configuration to route the incoming PSTN service DN call to the NRS and Avaya 3100 Mobile Communicator Gateway).
PSTN Service DN		The PSTN number that will be incoming to the enterprise that will be used for the service DN.
LDAP Server		
LDAP Search Base for users		
LDAP Username		
LDAP Password		
LDAP attribute tag that contains the user id		
LDAP attribute tag that contains the user's first name		
LDAP attribute tag that contains the user's last name		
LDAP attribute tag that contains the user's display name		

Configuration parameter	Value	Notes
LDAP attribute tag that contains the user's business phone #		
LDAP attribute tag that contains the user's mobile phone #		
LDAP attribute tag that contains the user's e-mail address		
LDAP attribute tag that contains the user's extension		
LDAP attribute tag that contains the user's home phone		

Avaya 3100 Mobile Communicator solution checklist

Use the following checklist to ensure that you have everything you need for the installation, commissioning, and interworking of your Avaya 3100 Mobile Communicator solution.

Table 19: Solution checklist

Item	Done?
Do all of the Avaya CS 1000 components have the latest deplist?	
Have all ISMs and packages been applied?	
Do you have an Avaya 3100 Mobile Communicator Gateway license?	
Prior to installation, do you have 2 CDs, one containing the Avaya CS 1000 Release and Linux Base, and one containing the latest Avaya 3100 Mobile Communicator Gateway build?	
Prior to installation, do you have a serial cable and a laptop to install the Avaya CS 1000 Linux base?	
Do you have the latest Avaya 3100 Mobile Communicator Gateway SU for the Avaya 3100 Mobile Communicator release you are installing?	
Do you have a program like putty (SSH) for telnet to the server command line? Do you have a program like Filezilla (SFTP) to FTP the SU to the platform?	
Does the Avaya 3100 Mobile Communicator Gateway TLAN have access to www.199.nortel.com (HTTP/TCP port 8008) to validate the Avaya 3100 Mobile Communicator Gateway license?	
After the Avaya 3100 Mobile Communicator Gateway is installed and running the release, have you applied the latest Avaya 3100 Mobile Communicator Gateway SU?	

Item	Done?
Have the firewall rules (if needed) been configured to allow Avaya 3100 Mobile Communicator clients access to port 8080 (HTTP) or 8443 (HTTPS) on the Avaya 3100 Mobile Communicator Gateway?	

Chapter 18: Appendix B: Call flows from CS 1000

The following figure shows the call flow for receiving an incoming call.

Avaya 3100 Mobile Communicator

Receiving an incoming call

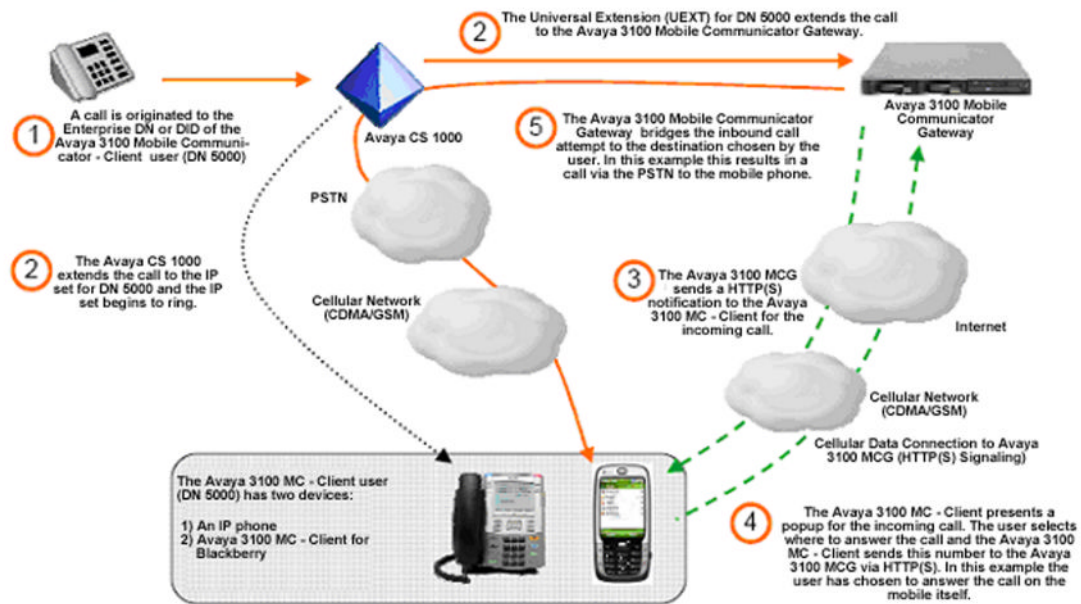


Figure 52: Receiving incoming call flow

The following figure shows the call flow for an outgoing call.

Avaya 3100 Mobile Communicator

Call Origination Mode #1 – Direct Mode

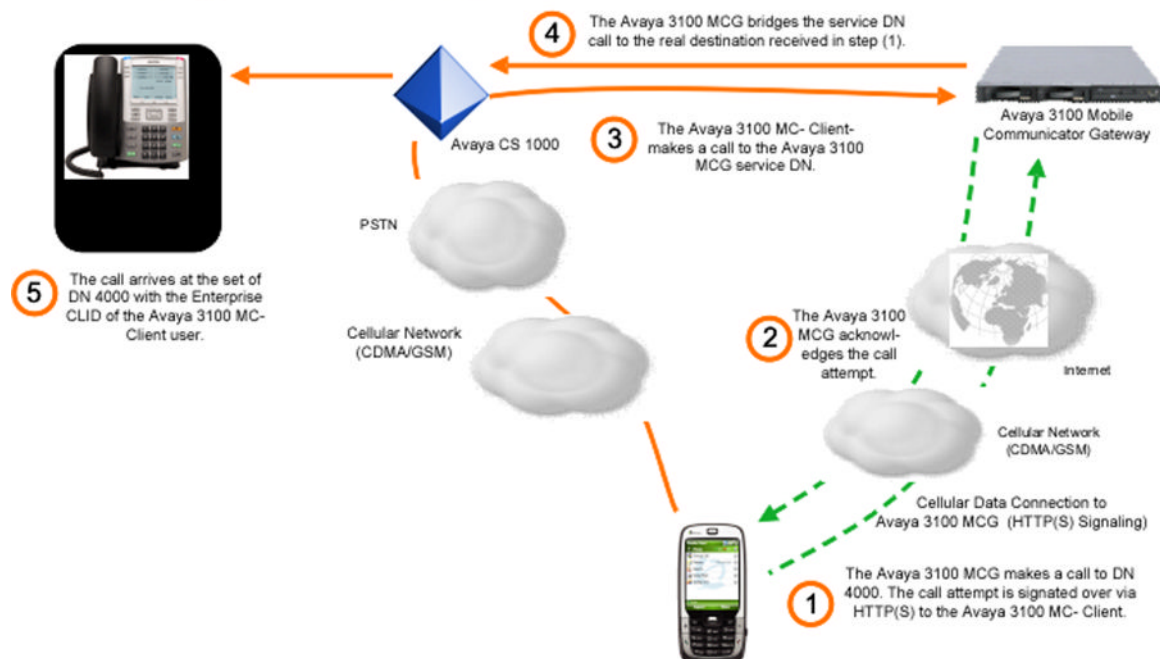


Figure 53: Outgoing call flow

Index

A

Avaya 3100 MC - Client for BlackBerry[13](#), [15](#), [16](#), [18](#),
[48](#)
 BlackBerry Enterprise Server (BES)[13](#), [15](#), [18](#)
 Dialing plan[16](#)
 Enterprise Call Server (ECS)[48](#)
Avaya 3100 MC - Client for Nokia[13](#), [16](#), [48](#)
 Dialing plan[16](#)
 Enterprise Call Server (ECS)[48](#)
 Virtual Private Network (VPN)[13](#)
Avaya 3100 MC - Client for Windows Mobile[13](#), [16](#),
[48](#)
 Dialing plan[16](#)
 Enterprise Call Server (ECS)[48](#)
 Virtual Private Network (VPN)[13](#)
Avaya 3100 MC - Web UI[13](#), [48](#)
 licenses[48](#)
Avaya 3100 Mobile Communicator Gateway . .[15](#), [18](#), [20](#),
[49](#)
 Enterprise Call Server (ECS)[15](#), [18](#), [49](#)
 High availability[20](#)
Avaya 3100 Mobility Communicator - Client

See Avaya 3100 MC - Client for Blackberry, Avaya
3100 MC - Client for Nokia, or Avaya 3100 MC -
Client for Windows Mobile

Avaya Communication Server 1000 (Avaya CS 1000)
 PSTN calculations[38](#), [39](#)
 SIP Access Ports calculations[38](#), [39](#)
 Universal Extension (UEXT) calculations[42](#)

B

BlackBerry Enterprise Server (BES)[13](#), [15](#), [18](#)

E

Enterprise Call Server (ECS)
 Dialing plan[16](#)

V

Virtual Private Network (VPN)[13](#)

